Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Robson Lima Lourenço

IMPLANTAÇÃO DO IPV6 NO SISTEMA AUTÔNOMO DO DECEx (DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO BRASILEIRO)

Rio de Janeiro

2013

Robson Lima Lourenço

IMPLANTAÇÃO DO IPV6 NO SISTEMA AUTÔNOMO DO DECEx (DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO BRASILEIRO)

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

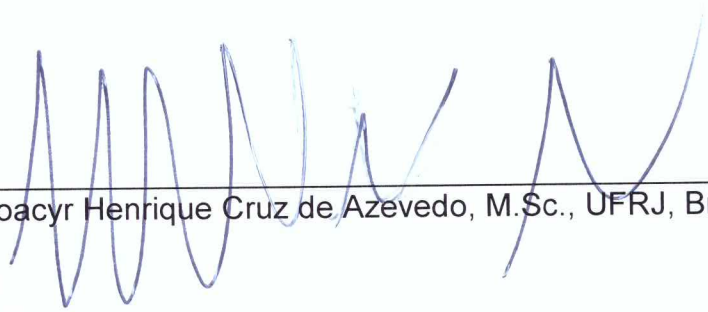
2013

Robson Lima Lourenço

IMPLANTAÇÃO DO IPV6 NO SISTEMA AUTÔNOMO DO DECEx (DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO BRASILEIRO)

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Dedico esta monografia a Deus por ter me proporcionado a concretização deste sonho me sustentando nos momentos mais difíceis, à minha esposa Beatriz Curvello Lourenço e filhos Ivan Curvello Lourenço e Artur Curvello Lourenço que se privaram da minha presença em vários momentos ao longo do curso.

AGRADECIMENTOS

Gostaria de agradecer ao DECEx (Departamento de Educação e Cultura do Exército) e à Fundação Roberto Trompowsky Leitão de Almeida na pessoa do Coronel Antônio Carlos Guelfi que proporcionou a realização deste curso e ao Tenente Coronel Mauro Macedo Machado que contribui grandemente em minha formação com suas orientações e paciência, e por ter disponibilizado recursos da instituição objeto deste estudo na hora de validá-lo.Agradeço ao Sargento Antônio Pinto Teixeira e aos companheiros administradores de rede da Fundação Trompowsky pelo apoio no acesso ao ambiente de teste. Agradeço ainda a minha esposa Beatriz pela sua dedicação e apoio durante todo o curso. Agradeço ao professor Moacyr Henrique Cruz de Azevedo pela sua orientação e paciência.

RESUMO

LOURENÇO, Robson Lima. **IMPLANTAÇÃO DO IPV6 NO SISTEMA AUTÔNOMO DO DECEX (DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO).** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Este trabalho tem como objetivo estudar o Protocolo de Internet que está evoluindo para a versão 6 (IPv6), suas características e peculiaridades comparadas ao IPv4, assim como seu adequado emprego avaliando as possibilidades de coexistência e técnicas de transição sempre com foco no cenário proposto que é um estudo de caso do Sistema Autônomo do Departamento de Educação e Cultura do Exército (DECEx). A necessidade de implantação do IPv6 se justifica devido ao iminente esgotamento dos endereços IPv4.

A IANA, órgão responsável pelo controle de distribuição dos endereços IP em todo o mundo, já não possui mais recursos a fornecer (IPv4) impossibilitando desta forma a expansão da Internet na forma que conhecemos. A implantação do IPv6 tem se mostrado a solução para todos os problemas encontrados no IPv4, como espaço de endereçamento, segurança, mobilidade, aplicações em tempo real e sobrecarga de roteadores. A quantidade de endereços quase infinita se destaca entre as características do novo IP.

ABSTRACT

LOURENÇO, Robson Lima. **IMPLANTAÇÃO DO IPV6 NO SISTEMA AUTÔNOMO DO DECEX (DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO).** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

This work aims to study the Internet Protocol that is evolving to version 6 (IPv6), its characteristics and peculiarities compared to IPv4, as well as its adequate job assessing the possibilities of coexistence and transition techniques always focusing on the proposed scenario that is a case study of the Autonomous System Department of Education and Culture of the Army (DECEX). The need for IPv6 deployment is justified due to the impending exhaustion of IPv4 addresses.

IANA, the body responsible for controlling the distribution of IP addresses around the world, no longer has to provide more resources (IPv4) thus preventing the expansion of the Internet as we know. The deployment of IPv6 has been shown to be the solution to all problems found in IPv4, such as address space, security, mobility, real-time applications and routers overhead. More addresses almost endless stands out among the features of the new IP.

LISTA DE FIGURAS

Página

LISTA DE TABELAS

Página

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ALG	Application Layer Gateway
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ASN	Autonomous Sytem Number
AT&T	American Telephone and Telegraph
BGP	Border Gateway Protocol
BIA	Bump in the API
BIND	Berkeley Internet Name Domain ou Berkeley Internet Name Daemon
BIS	Bump in the Stack
CATNIP	Common Architecture for Next-generation Internet Protocol
CGI	Comitê Gestor da Internet no Brasil
CIDR	Classless Inter-Domain Routing
DECEx	Departamento de Educação e Cultura do Exército Brasileiro
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS-ALG	Domain Name System - Application Layer Gateway
EBNET	Rede Corporativa do Exército
EGP	Exterior Gateway Protocol
EMBRATEL	Empresa Brasileira deTelecomunicações
EUI	Extended Unique Identifier
GRE	Generic Routing Encapsulation)
HP	Hewlett-Packard
HTTP	HyperText Transfer Protocol
IAMA	Internet Assigned Numbers Authority
IBM	International Business Machines
ICMPV6	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPNWG	*IPNext Generation Working Group*
IPplan	IP address management and tracking
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
IPX	Internal Packet eXchange
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO	International Organizational for Standardization
ISP	Internet Service Provider
LACNIC	Registro de Endereços da Internet para a América Latina e o Caribe
LSA	Link State Advertisement

LTS	Long Term Support
MAC	Media Access Control
MIT	Massachusetts Institute of Technology
MLD	Multicast Listener Discovery
MPLS	Multi Protocol Label Switching
MPOG	Ministério do Planejamento, Orçamento e Gestão
MTR	Matt's Traceroute
MTU	Maximum Transit Unit
MX	Mail eXchange
NAT	Network Address Translation
ND	Neighbor Discovery
NIC.BR	Núcleo de Informação e Coordenação do Ponto BR
NS	Name Server
NSAP	Network Service Access Point address
OMDS	Organizações Militares Diretamente Subordinadas
OSI	*Open Systems Interconnection*
OSPF	Open Shortest Path First
PIX	Ponto de Interconexão ou ponto de acesso ao PTTMetro.
POP-RJ	Ponto de Presença da RNP no Rio de Janeiro
PTTMETRO	Pontos de Troca de Tráfego Metropolitanos
RA	Router Advertisement
RAM	Random Access Memory
RFC	Request for Comments
RIR	Regional Internet Registry
RNP	Rede Nacional de Pesquisa
RP	Responsible Person
RS	Router Solicitation
SIIT	Stateless IP/ICMP Translation Algorithm
SIPP	Simple Internet Protocol Plus
SixXS	*Six Access*
SOA	Start of Authority
TCP	*Transmission Control*
TRT	Transport Relay Translator
TTL	Time to Live
TUBA	TCP and UDP with Bigger Addresses
UDP	User Datagram Protocol
ULA	Unique Local Address

SUMÁRIO

1 **INTRODUÇÃO**

A Grande Rede Mundial de Computadores, como é conhecida a Internet, vem sofrendo evoluções e crescimentos vertiginosos desde a sua criação a cerca de 30 anos atrás quando foi criada pela ARPANET (*Advanced Research Projects Agency Network),* que tinha como objetivo inicial criar uma estrutura de intercomunicação que pudesse manter a troca de informações, ainda que uma parte da rede fosse danificada.

Essa Rede foi se expandindo para interligar universidades facilitando a comunicação entre os seus cientistas e consequentemente sendo aprimorada até o formato em que conhecemos hoje. Essa grande evolução e expansão da Internet que experimentamos hoje, certamente, só é possível por causa do TCP/IP (*Transmission Control / Internet Protocol)* que foi originado com base no modelo de camadas da ISO (*International Organizational for Standardization)* que criou o modelo de referência OSI (*Open Systems Interconnection) em1977.*

Com o já mencionado super crescimento da Internet devido à sua popularização de acesso, com redes (super rápidas) com largura de banda cada vez maior, com computadores pessoais de alto poder de processamento e também com conteúdos cada vez mais atraentes a todos os públicos, percebeu-se que um grande problema estava por acontecer: a Internet que se conhece hoje está num ritmo de crescimento que em breve alcançará seu limite. Originalmente não foi projetada para dar suporte a uma rede de tamanho tão gigantesco que alcançou, logo, a distribuição de endereços IPv4 já está se esgotando devido a falhas no projeto da concepção do protocolo. Falhas do tipo excessiva alocação de espaço de endereçamento, como dezenas de faixas classe A que foram integralmente cedidas a grandes instituições tais quais IBM, AT&T, Xerox, HP, Apple, MIT, Ford,

Departamento de Defesa Americano, entre várias outras, disponibilizando dessa forma 16.777.216 milhões de endereços para cada uma. E ainda, 35 faixas de endereços classe A foram reservadas para usos específicos como *multicast, loopback* e uso futuro.

Em 1990 já haviam 313.000 *hosts* conectados à rede e outros problemas também começaram a surgir como o enorme aumento das tabelas de roteamento.

Três anos mais tarde surgiu o protocolo HTTP (*HyperText Transfer Protocol*) e também a liberação pelo governo Norte Americano para a utilização da Internet de forma comercial, provocando um grande pico no crescimento da rede, que pulou de 2.056.000 *hosts* em 1993 para mais de 26.000.000 de *hosts* em 1997.

Atualmente a IANA (*Internet Assigned Numbers Authority*) que é responsável pela coordenação global do DNS raiz, do endereçamento IP, e outros recursos do protocolo Internet, não possui mais blocos de endereçamento IP para fornecer, tendo sido todos distribuídos para instituições como as já mencionadas e seus representantes regionais conforme a divisão apresentada na Figura 1.

Figura 1 – Mapa dos Registros Regionais de Internet.

Diante do caos iminente, em 1993 o IETF (*Internet Engineering Task Force*) criou um grupo de trabalho para uma nova versão do protocolo IP, o IPngWG (*IPNext Generation Working Group*). O grupo de trabalho selecionou então três protocolos para a camada de rede da arquitetura TCP/IP (CATNIP, TUBA e SIPP). O protocolo SIPP (*Simple Internet Protocol Plus*) foi o indicado pelo grupo por ser o que mais se assemelhava com o IPv4. Porém a soma dos aspectos positivos de cada um dos três protocolos foi utilizada gerando, assim, a proposta para uma versão 6 do protocolo de Internet.

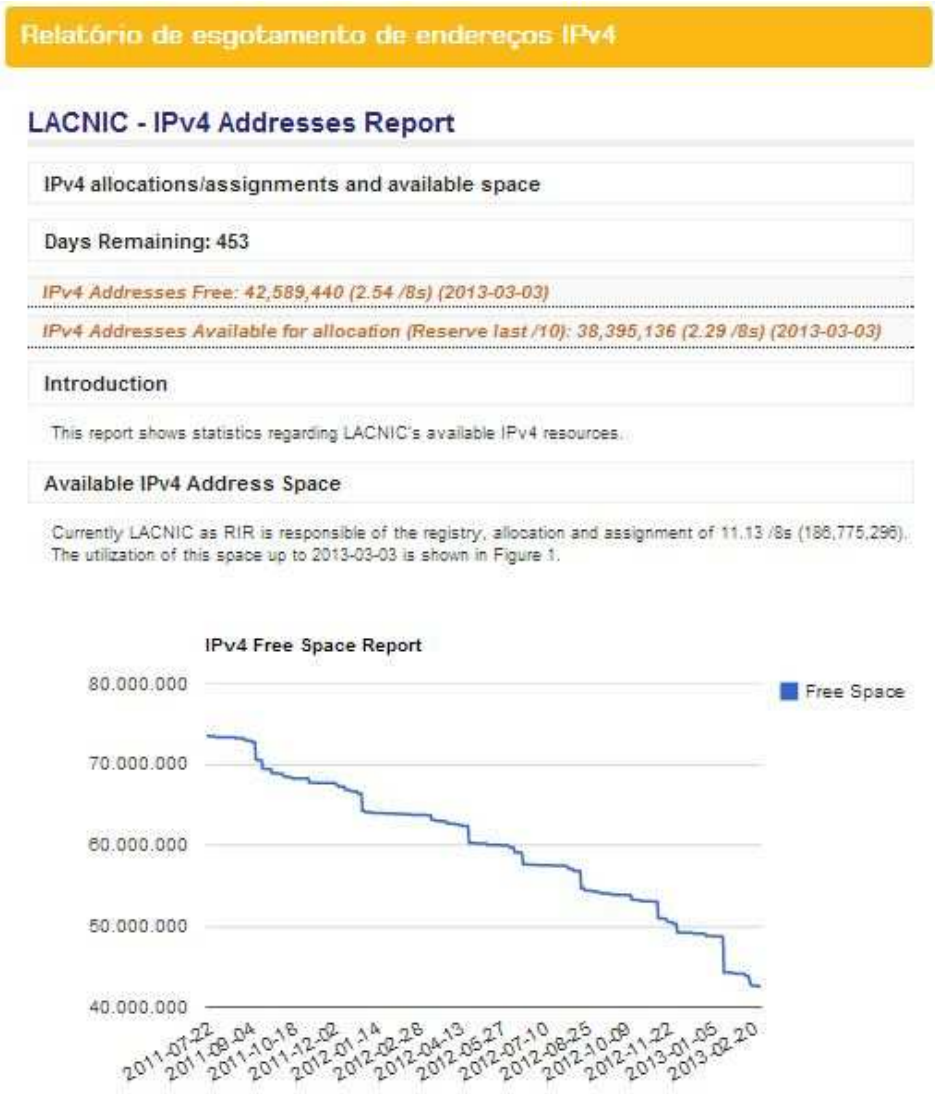


Figura 2 – Previsão de Esgotamento do IPv4 no âmbito do LACNIC.

Na Figura 2 é possível observar um relatório atualizado da quantidade de endereços IP ainda disponíveis no RIR (*Regional Internet Registry*) responsável pela região da América Latina e Caribe, o LACNIC.

Este trabalho tem como objetivos apresentar o IPv6 sugerindo boas práticas de implantação em um ambiente corporativo, baseado em experiências acumuladas por ocasião da implantação do novo protocolo de Internet no AS (*Autonomous System*) do DECEx (Departamento de Educação e Cultura do Exército Brasileiro).

2 **O PROTOCOLO DE INTERNET VERSÃO 6 (IPv6)**

2.1 PRINCIPAIS CARACTERÍSTICAS

O IPv6 oferece uma série de melhorias comparado ao seu antecessor, dos quais destacam-se os seguintes :

- Maior capacidade para endereçamento, aumentando de 32 bits (4.294.967.296 endereços possíveis) exclusive os reservados, para 128 bits (79 trilhões de trilhões de vezes o espaço disponível no IPv4);
- Simplificação do formato do cabeçalho reduzindo o custo do processamento dos pacotes nos roteadores;
- Suporte a cabeçalhos de extensão permitindo um roteamento mais eficaz;
- Capacidade de identificar fluxos de dados, adicionando um novo recurso que possibilita a identificação de determinados tráfegos de fluxos, possibilitando tratamentos especiais de acordo com a necessidade;
- Suporte a autenticação e privacidade, através de cabeçalhos de extensão capazes de fornecer mecanismos de autenticação, garantindo assim a integridade e confidencialidade dos dados transmitidos.

2.2 O DATAGRAMA IPv6

O datagrama IPv6 foi simplificado permanecendo apenas com oito campos e com tamanho fixo de 40 bytes, fazendo uso de extensões por meio de cabeçalhos adicionais, quando houver necessidade, tornando-o flexível, eficiente, e evitando o processamento em todos os roteadores intermediários. As mudanças ocorridas proporcionaram um crescimento de apenas duas vezes o tamanho do cabeçalho IPv4, apesar de possuir um espaço de endereçamento quatro vezes maior.

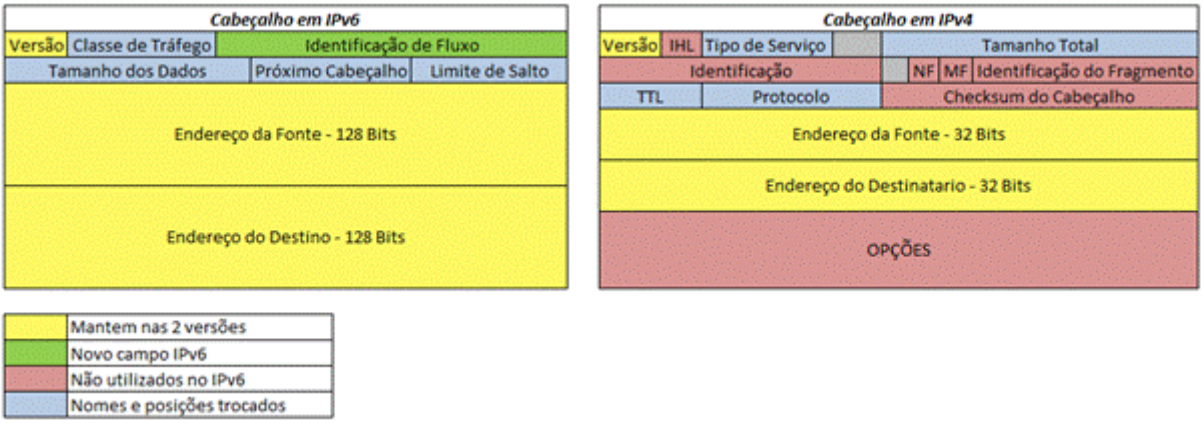


Figura 3 - Cabeçalho dos Protocolos IPv4 e IPv6 e suas alterações

Seis campos do cabeçalho IPv4 foram removidos e outros quatro campos tiveram seus nomes alterados e seus posicionamentos modificados.

Os campos removidos foram:

- Opções e Complemento – as opções adicionais agora fazem parte dos cabeçalhos de extensão do IPv6;
- Tamanho do Cabeçalho – o tamanho do cabeçalho IPv6 agora é fixo;
- Identificação – as informações de fragmentação agora são tratadas em um cabeçalho de extensão apropriado;
- Flag – pelo fato do IP não ser um serviço confiável (sem dar garantia de entrega), para que o equipamento de destino saiba que recebeu o último fragmento do datagrama orginal, o último datagrama tem um bit setado para 0 (zero), enquanto que os outros fragmentos têm o bit de flag setado para 1. Essas informações de fragmentação agora são tratadas em um cabeçalho de extensão apropriado;
- Deslocamento do Fragmento – as informações de fragmentação agora são tratadas em um cabeçalho de extensão apropriado;

- Soma de verificação (*Checksum*) – foi removido para aumentar a velocidade do processamento dos roteadores, pois o cálculo já é feito nas camadas superiores.

Os campos que tiveram seu nome e posicionamento alterados são os seguintes:

- Tipo de Serviço – passou a se chamar Classe de Tráfego;
- Tamanho Total – passou a se chamar Tamanho dos Dados;
- Tempo de Vida (TTL) – passou a se chamar Limite de Encaminhamento;
- Protocolo – passou a se chamar Próximo Cabeçalho.

Desta forma o cabeçalho IPv6 passou a contar com os seguintes campos:

- Versão (4 bits) – Identifica a versão do protocolo IP utilizado, no caso o valor do campo é 6;
- Classe de Tráfego (8 bits) – Identifica e diferencia pacotes por classes de serviços ou prioridade;
- Identificador de Fluxo (20 bits) – É usado em conjunto com o campo de endereço de origem para identificar fluxo de tráfego na rede;
- Tamanho dos Dados (16 bits) – Este campo substituiu o campo chamado Tamanho Total do IPv4. É empregado para informar em bytes apenas os dados enviados junto ao cabeçalho IP;
- Próximo Cabeçalho (8 bits) – Este campo foi renomeado, no IPv4 chamava-se Protocolo. Armazena a identificação do tipo de cabeçalho que segue o cabeçalho básico do IP (cabeçalhos adicionais);
- Limite de Encaminhamento (8 bits) – Informa o número máximo de roteadores que o pacote IP pode atravessar antes de ser descartado;
- Endereço de Origem (128 bits) – Indica o endereço de origem do pacote;

- Endereço de Destino (128 bits) - Indica o endereço destino do pacote.

2.3 ENDEREÇAMENTO

O protocolo IPv6 tem como principal característica o aumento no espaço de endereçamento. Será visto a partir de agora as diferenças entre os endereços IPv4 e IPv6 e suas características.

Um endereço IPv4 é formado por 32 bits, o que significa:

2^{32} = 4.294.967.296 de endereços

Um endereço IPv6 é formado por 128 bits, o que significa:

2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456

~ 56 octilhões (5,6 x 10^28) de endereços IP por ser humano.

~ 79 octilhões (7,9 C 10^28) de vezes a quantidade de endereços IPv4.

Os endereços IPv6 são representados através de oito grupos de 16 bits, separados por “ **:** ” e escritos com caracteres hexadecimais.

Exemplo:

2001:0BDA:ADF1:2E45:CAFE:FACA:CADE:0123

2 bytes

Ao se escrever um endereço IPv6 é possível:

- Usar caracteres minúsculos ou maiúsculos;
- Deixar de representar os zeros à esquerda; e
- Substituir os zeros contínuos por “ **::** ” (somente uma vez).

Exemplo:

2001:DA0:0000:0000:230F:0000:0000:130F

2001:da0:0:0:230f::130f

Formato errado: 2001:da0**::**230f**::**130f (gera ambiguidade)

Representação dos Prefixos:

Assim como o CIDR (*Classless Inter-Domain Routing*) do IPv4 também irá adotar o modelo “Endereço-IPv6/Tamanho do Prefixo”

Exemplo:

Prefixo 2001:deb:1001:2::/64

Prefixo Global 2001:deb::/32

ID da Sub-rede 1001:2

De todo espaço de endereçamento do IPv6, somente 15% foi previsto para uso conforme apresentado no quadro 1, sobrando portanto 85% que ficou reservado para o futuro.

Quadro 1 - Alocação do Espaço de Endereçamento

ALOCAÇÃO	**PREFIXO** (binário)	**FRAÇÃO DO ESPAÇO DE ENDEREÇAMENTO**
Reservado	0000 0000	1/256
Não Alocado	0000 0001	1/256
Reservado para Alocação	0000 001	1/128
Reservado para Alocação	0000 010	1/128
Não Alocado	0000	1/128
Não Alocado	0000	1/32
Não Alocado	0001	1/16
Aggregatable Global	001	1/8
Não Alocado	010	1/8
Não Alocado	011	1/8
Não Alocado	100	1/8
Não Alocado	101	1/8
Não Alocado	110	1/8
Não Alocado	1110	1/16
Não Alocado	1111 0	1/32

ALOCAÇÃO	**PREFIXO** (binário)	**FRAÇÃO DO ESPAÇO DE ENDEREÇAMENTO**
Não Alocado	1111 10	1/64
Não Alocado	1111 110	1/128
Não Alocado	1111 1110 0	1/512
Site-local Unicast Address	1111 1110 10	1/1024
Link-local Unicast Address	1111 1110 11	1/1024
Multicast Address	1111 1111	1/256

2.4 TIPOS DE ENDEREÇO

Existem na arquitetura de endereços IPv6 essencialmente três tipos de endereços: *Unicast*, *Anycast e Multicast*. Não existe mais o *Broadcast* no IPv6, porém sua funcionalidade passou a ser suportada pelos endereços *Multicast.*

2.4.1 **Endereços *Unicast***

Os endereços *unicast* são considerados de identificação única. Um pacote que tenha sido destinado a um determinado endereço *unicast* será enviado diretamente para a interface associada àquele endereço. Os endereços *unicast* ainda foram classificados em: *Aggregatable Global Unicast Address, Unspecified Address, Loopback Address, Embedded IPv4 Address, NSAP Address, IPX Address e Local-Use IPv6 Address.*

2.4.1.1 Aggregatable Global Unicast Address

Os endereços *Global Unicast,* como são mais conhecidos, são equivalentes aos endereços públicos do IPv4, globalmente roteáveis e acessíveis na Internet IPv6.

Sua estrutura foi projetada para utilizar os 64 bits mais a esquerda para identificar a rede e os 64 bits restantes para identificação da interface. Consequentemente, todas as redes possuem o mesmo tamanho de prefixo, 64 bits (/64), possibilitando o endereçamento de 2^{64} de hosts por subrede.

2.4.1.2 *Unspecified Address*

Representado por 0:0:0:0:0:0:0:0 ou "::0". Esse endereço nunca deve ser atribuído a nenhum host, é utilizado apenas para indicar a ausência de endereço. É geralmente utilizado no campo Endereço de Origem de um pacote IPv6 durante a inicialização de um host que ainda não tenha seu endereço definido.

2.4.1.3 *Loopback Address*

Endereço representado por 0:0:0:0:0:0:0:1 ou "::1" (equivalente ao endereço *loopback* IPv4 127.0.0.1). Geralmente empregado para referenciar o próprio host, sendo utilizado para testes internos. Não deve ser associado a nenhuma interface física, seja como endereço de origem ou de destino, mas pode ser imaginado como sendo de uma interface virtual (*loopback*). Um pacote com o endereço *loopback* como destino não deve ser encaminhado por um roteador IPv6. Da mesma forma, um pacote que chegue a alguma interface com o endereço de *loopback* como destino deve ser descartado.

2.4.1.4 *Embedded IPv4 Address*

Refere-se a um endereço IPv6 com um endereço IPv4 embutido. Também conhecido como *IPv4-compatible IPv6 Address***.** É composto atribuindo-se um prefixo nulo com 96 bits de zeros e o endereço IPv4. Esta notação (::201.13.28.15) foi criada como mecanismo de transição para que *hosts* e roteadores pudessem tunelar pacotes IPv6 sobre roteamentos IPv4.

Também foi definido um outro tipo de endereço para *hosts* sem suporte a IPv6 utilizando o *IPv4-mapped IPv6 Address* da seguinte forma: 0:0:0:0:0:FFFF:ABCD ou ::FFFF:ABCD. É utilizado para mapear um endereço IPv4 dentro de um endereço IPv6 de 128 bits, onde ABCD representam os 32 bits do endereçamento IPv4,

utilizando-se dígitos decimais. Também empregado com técnica de transição para que nós IPv6 e Ipv4 possam se comunicar. Ex.: ::FFFF:172.16.10.1

2.4.1.5 *NSAP Address*

O *NSAP Address* é identificado como tendo o primeiro byte do endereço começando pelos bits 0000001 (prefixo de 121 bits) para fornecer um meio de mapear os endereços de ponto de acesso a serviços de rede (NSAP) para endereços IPv6.

2.4.1.6 *IPX Address*

Os endereços IPX (*Internal Packet eXchange*) são utilizados em redes Netware e são identificados pelo prefixo de 121 bits 0000010. Foram incluídos para mapear endereços IPX em endereços IPv6.

2.4.1.7 *Local-Use IPv6 Address*

Existem dois tipos de endereços para uso local: *Link-local e Unique Local Address* (ULA)*:*

2.4.1.7.1 *Link-local*

Um endereço do tipo *Link-local* pode ser utilizado somente na rede onde a interface estiver conectada, o endereço é fornecido automaticamente utilizando o prefixo FE80::/64. Os 64 bits reservados para identificação da interface são configurados com base no padrão IEEE EUI-64. Os roteadores não devem encaminhar para outros enlaces pacotes que tenham como origem ou destino um endereço do tipo *Link-local.*

2.4.1.7.2 *Unique Local Address* (ULA)

Trata-se de um endereço com grande possibilidade de ser globalmente único, deve ser utilizado para comunicações dentro de um mesmo enlace ou conjunto de enlaces. Este tipo de endereço pode ser considerado como privado, visto que está

confinado a um domínio sem acesso à Internet. Esse tipo de endereço não pode ser roteado ou anunciado na Internet. Pode ser identificado pelo prefixo FC00::/7 .

2.4.2 **Endereços *Anycast***

Os endereços *anycast* são atribuídos a mais de uma interface que geralmente pertencem a nós diferentes. Quando um pacote é enviado a um endereço *anycast* ele é roteado para a interface mais próxima com o endereço configurado, de acordo com a medida de distância empregada comumente pelos roteadores. Outros usos possíveis de endereços *anycast* seriam identificar um conjunto de roteadores que fazem parte de uma sub-rede particular, ou o conjunto de roteadores de entrada para um domínio específico. Os endereços *anycast* são alocados a partir do espaço de endereço do *unicast*, usando alguns dos formatos de endereço definidos para o *unicast*. Assim, os endereços *anycast* são indistintos dos endereços *unicast.*

2.4.3 **Endereços *Multicast***

Assim como o *anycast*, os endereços *multicast* são designados para identificar um conjunto de interfaces de diferentes hosts, porém quando um pacote for enviado a um endereço *multicast* este deverá ser encaminhado a todas as interfaces de rede associadas a este endereço. O *multicast* assumiu algumas funções que eram do *broadcast*, tendo em vista este não existir mais no IPv6.

2.5 SERVIÇOS BÁSICOS DO IPv6

2.5.1 **ICMPv6**

O ICMPv6 (*Internet Control Message Protocol*) é um protocolo fundamental na arquitetura IPv6, visto que, além do gerenciamento *multicast,* através do protocolo MLD (*Multicast Listener Discovery*), e da resolução de endereços da camada dois, suas mensagens são de suma importância para o funcionamento do protocolo de Descoberta de Vizinhança (*Neighbor Discovery)*, responsável por localizar

roteadores vizinhos na rede, detectar mudanças de endereço no enlace e detectar endereços duplicados. Com relação à mobilidade, o cabeçalho de extensão *Destination Options* é utilizado no suporte ao mecanismo de mobilidade do IPv6 através da opção *Home Address*, que contém o endereço de origem do nó móvel quando este está em trânsito.

2.5.2 ***Neighbor Discovery*** (ND)

O *Neighbor Discovery* é um protocolo do IPv6 que utiliza as mensagens do ICMPv6 para executar funções agregadas que antes eram executadas pelo ARP, ICMP *Router Discovery e ICMP Redirect to* IPv4. Portanto, são funções do ND:

a) Determinar endereço MAC de *hosts* vizinhos;

b) Encontrar roteadores para encaminhamento de pacotes;

c) Manter registros atualizados de *hosts* vizinhos;

d) Detectar endereços duplicados;

e) Autoconfiguração de endereços.

O IPv6 implementa uma funcionalidade que não existia no IPv4, a autoconfiguração de endereços sem a dependência de um servidor DHCP (*Dynamic Host Configuration Protocol*). Com essa característica fica mais simplificada a conexão de novos equipamentos à Internet, como celulares e aparelhos domésticos.

O *host* envia uma mensagem *Router Solicitation* ao grupo *multicast all-routers,* então todos os roteadores do enlace respondem com uma mensagem *Router Advertisement* informando: os roteadores padrão; um valor predefinido para o campo Limite de Encaminhamento; o MTU (*Maximum Transit Unit)* do enlace e a lista de prefixos da rede para os quais também serão gerados endereços automaticamente.

3 **O DECEx (Departamento de Educação e Cultura do Exército)**

O Departamento de Educação e Cultura do Exército gerencia o patrimônio histórico e cultural da Força Terrestre. Além disso, o DECEx é o órgão central de um amplo sistema que abrange o ensino nas suas mais diferentes matizes, aprimorando a qualidade do profissional militar e do cidadão para bem servir à Força Terrestre e à Nação.

Tem por objetivo conduzir, no âmbito do Exército, as atividades relativas aos assuntos culturais, educação física e desportos, ao ensino e à pesquisa e ao desenvolvimento, nas áreas de doutrina e pessoal.

O departamento objeto deste estudo acata a diretriz do Governo Federal de se utilizar essencialmente aplicações *Open Source,* conforme descrito no site do Ministério do Planejamento, Orçamento e Gestão [MPOG, 2013].

3.1 TOPOLOGIA

A título de informação a figura 4 apresenta a grandeza e complexidade da rede do DECEx que possui vários enlaces de dados interligando suas OMDS (Organizações Militares Diretamente Subordinadas) e escolas. Não se pretende neste trabalho entrar em muitos detalhes da topologia por se tratar de dado sensível do referido departamento e sua política de segurança da informação não permitir tal divulgação.

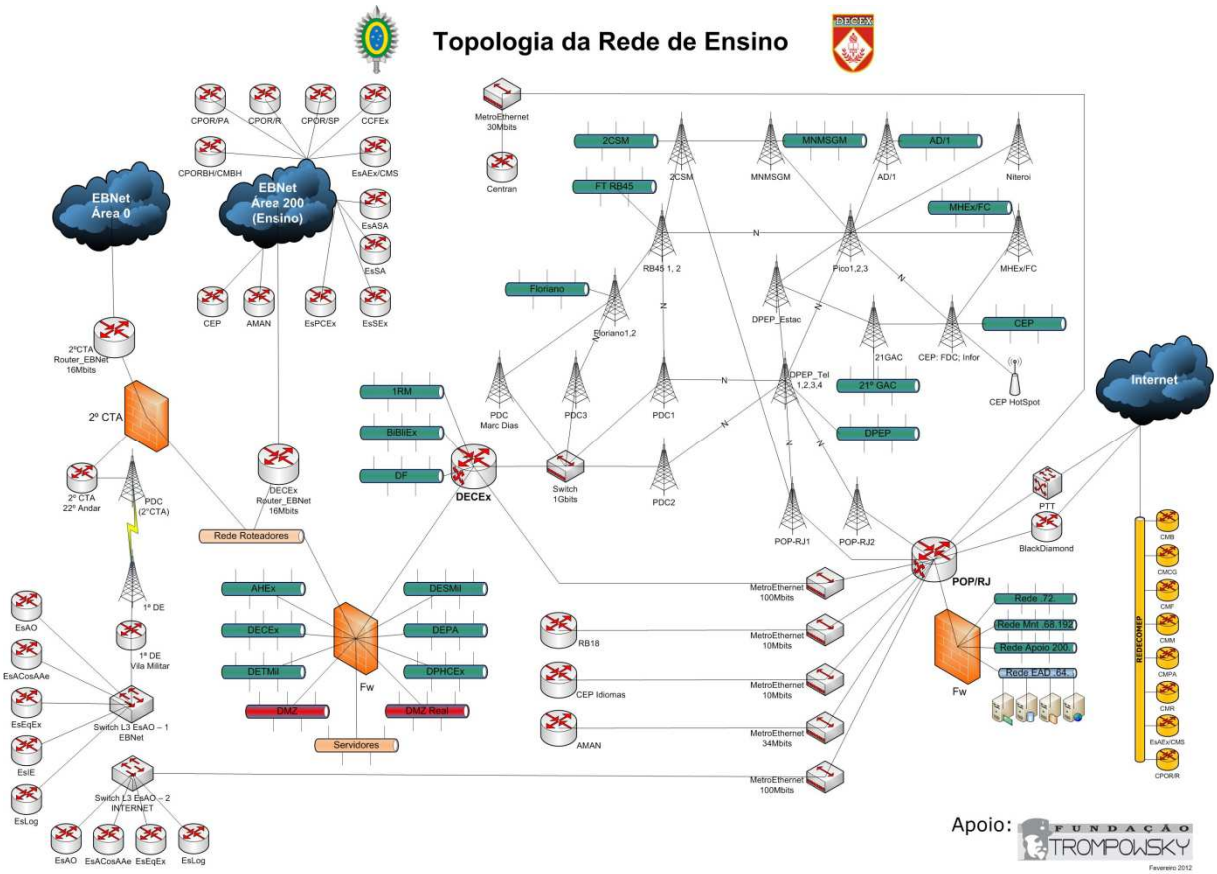


Figura 4 – Topologia da Rede de Ensino do DECEx

3.2 INFRAESTRUTURA

O DECEx dispõe de uma grande infraestrutura para poder prover todos os serviços que se propõe a executar e, para tanto, faz uso dos recursos humanos da Fundação Roberto Trompowsky Leitão de Almeida de Apoio ao DECEx, com mão-de-obra altamente qualificada em seus quadros, tendo em vista não possuir efetivo em quantidade ou habilidades suficientes. O departamento possui diversas escolas militares espalhadas por todo o território nacional que se ligam a matriz, que fica localizada no Palácio Duque de Caxias, Centro do Rio de Janeiro, por intermédio da rede integrada de serviços de comunicação de voz, dados e imagens. A Rede Corporativa do Exército, chamada de EBNet, que é provida pela EMBRATEL em

MPLS. As velocidades dos enlaces variam entre 2 e 16 Mbps dependendo de uma região para outra.

Por ser classificado como Instituição de Ensino e Pesquisa o DECEx possui acordo de cooperação com a Rede Nacional de Pesquisa (RNP) e está ligado ao Ponto de Presença da RNP no Rio de Janeiro (PoP-RJ), que fica em Botafogo, via enlace de dados Metro Ethernet de 100Mbps. Usufruindo assim da infraestrutura do DataCenter do PoP-RJ, hospedando vários de seus servidores, com no-breaks de 60 e 80 KVA, gerador de 150 KVA, ambiente refrigerado, conexão de 10Gbps ao *backbone* da RNP, conforme a Figura 5, e saída para Internet de 4Gbps.

Como o DECEx já possuía um *Autonomous System* (AS) bastou fazer a solicitação de um bloco IPv6 ao órgão regulador da internet no Brasil, o Comitê Gestor da Internet no Brasil (CGI), por intermédio de um procedimento padrão de justificativa de uso.

3.2.1 **O Sistema Autônomo**

O DECEx possui um Sistema Autônomo. Um Sistema Autônomo (SA) é um grupo de redes e roteadores IP abaixo de uma única gerência técnica e que compartilham uma mesma política de roteamento [Hawkinson e Bates, 1996]. O roteamento dentro de um AS é denominado de roteamento interno. O roteamento entre os AS é denominado de roteamento externo. Cada AS pode adotar um protocolo de roteamento interno que desejar dentro do próprio AS, no caso é empregado o OSPF (*Open Shortest Path First***)**. Entretanto inter-AS é permitido somente um protocolo de roteamanto externo, o BGP (*Border Gateway Protocol***)**. O seu ASN (*Autonomous Sytem Number*) é o 28301 e ao solicitar um bloco IPv6 recebeu o prefixo 2801:80:d0::/48 possibilitando dar início ao planejamento de implantação do novo protocolo.

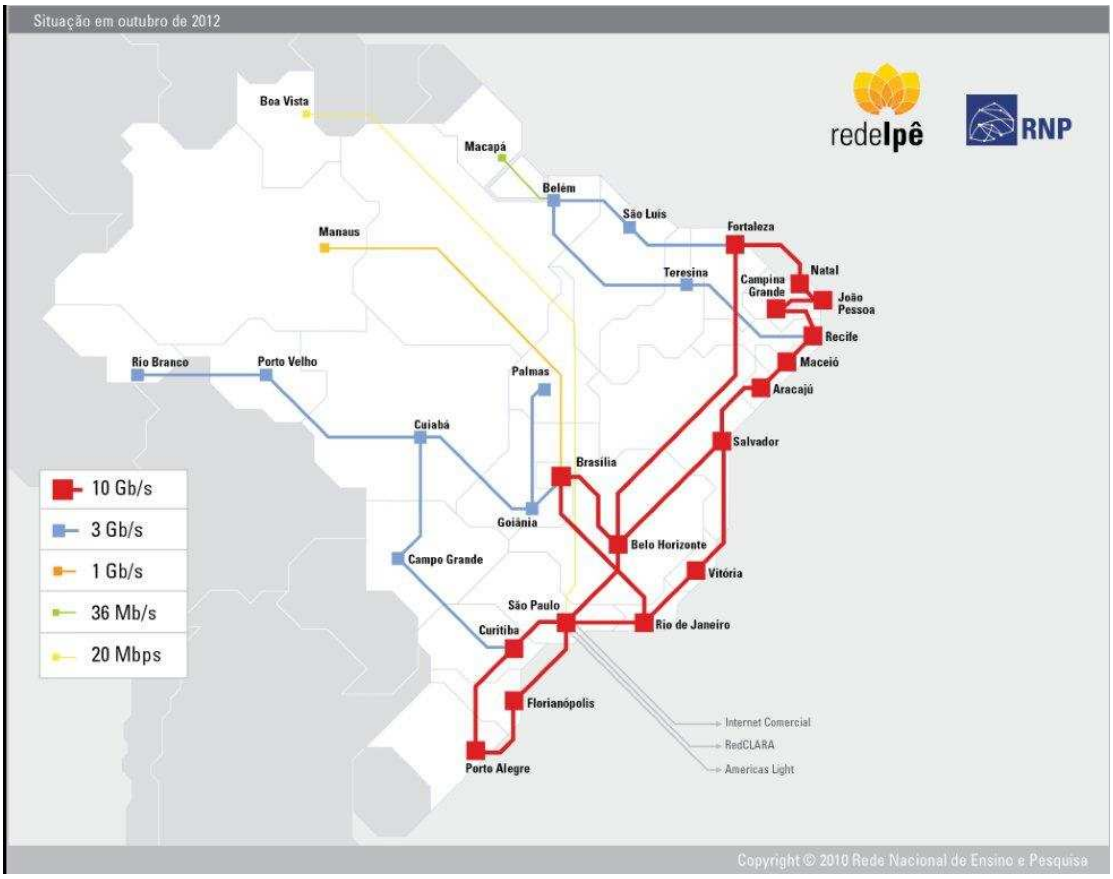


Figura 5 – *Backbone* da RNP

3.2.2 **O PTTMetro**

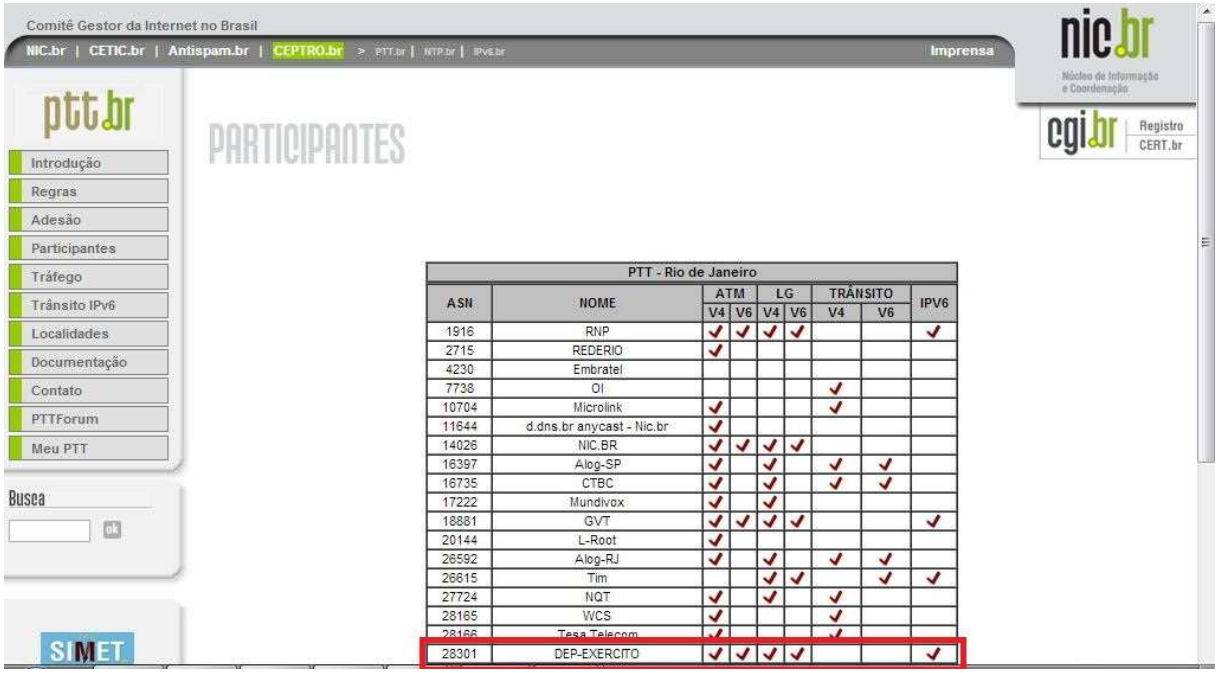
PTTMetro é o nome dado ao projeto do Comitê Gestor da Internet no Brasil (CGIbr) que promove e cria a infra-estrutura necessária (Ponto de Troca de Tráfego - PTT) para a interconexão direta entre os *Autonomous Systems* (ASs) que compõem a Internet Brasileira. O PTTMetro é destinado às regiões metropolitanas no País que apresentam grande interesse de troca de tráfego Internet.

Uma das principais vantagens deste modelo é a racionalização dos custos, uma vez que os balanços de tráfego são resolvidos direta e localmente e não através de redes de terceiros, muitas vezes fisicamente distantes.

Outra grande vantagem é o maior controle que uma rede pode ter com relação a entrega de seu tráfego o mais próximo possível do seu destino, o que em

geral resulta em melhor desempenho e qualidade para seus clientes e operação mais eficiente da Internet como um todo.

Um PTTMetro é, assim, uma interligação em área metropolitana de pontos de interconexão de redes (PIXes), comerciais e acadêmicas, sob uma gerência centralizada.



PTT - Rio de Janeiro

ASN	NOME	ATM		LG		TRÂNSITO		IPV6
		V4	V6	V4	V6	V4	V6	
1916	RNP	✓	✓	✓	✓			✓
2715	REDERIO	✓						
4230	Embratel							
7738	OI					✓		
10704	Microlink	✓				✓		
11644	d.dns.br anycast - Nic.br	✓						
14026	NIC.BR	✓	✓	✓	✓			
16397	Alog-SP	✓		✓		✓	✓	
16735	CTBC	✓		✓		✓	✓	
17222	Mundivox	✓		✓				
18881	GVT	✓	✓	✓	✓			✓
20144	L-Root	✓						
26592	Alog-RJ	✓		✓		✓	✓	
26615	Tim			✓	✓		✓	✓
27724	NQT	✓		✓		✓		
28165	WCS	✓				✓		
28166	Tesa Telecom	✓				✓		
28301	DEP-EXERCITO	✓	✓	✓	✓			✓

Figura 6 - Participantes do PTTMetro RJ

4 **POLÍTICA DE ALOCAÇÃO E DESIGNAÇÃO DO IPv6**

Cada RIR recebe da IANA um bloco /12 . A alocação 2800::/12 corresponde ao espaço reservado para o LACNIC e o NIC.br trabalha com um /16 que faz parte desse /12. A alocação mínima para um ISP (*Internet Service Provider)* é um bloco /32, mas, alocações maiores podem ser feitas mediante apresentação de justificativa de utilização.

4.1 RECOMENDAÇÕES PARA DESIGNAÇÃO DE ENDEREÇOS

Seguindo as orientações da RFC3177 as redes /48 são recomendadas para todo tipo de usuário, seja doméstico, pequeno ou grande. Empresas com grandes necessidades justificadas podem receber um /47, prefixos menores, ou mais de um /48. O /64 é recomendado para quando se tiver certeza que somente uma sub-rede é requerida. Uma rede /128 pode ser utilizada quando existir absoluta certeza que somente uma interface será conectada. Na Figura 7 é possível ver o espaço de endereçamento e suas subdivisões de acordo com a política da IANA.

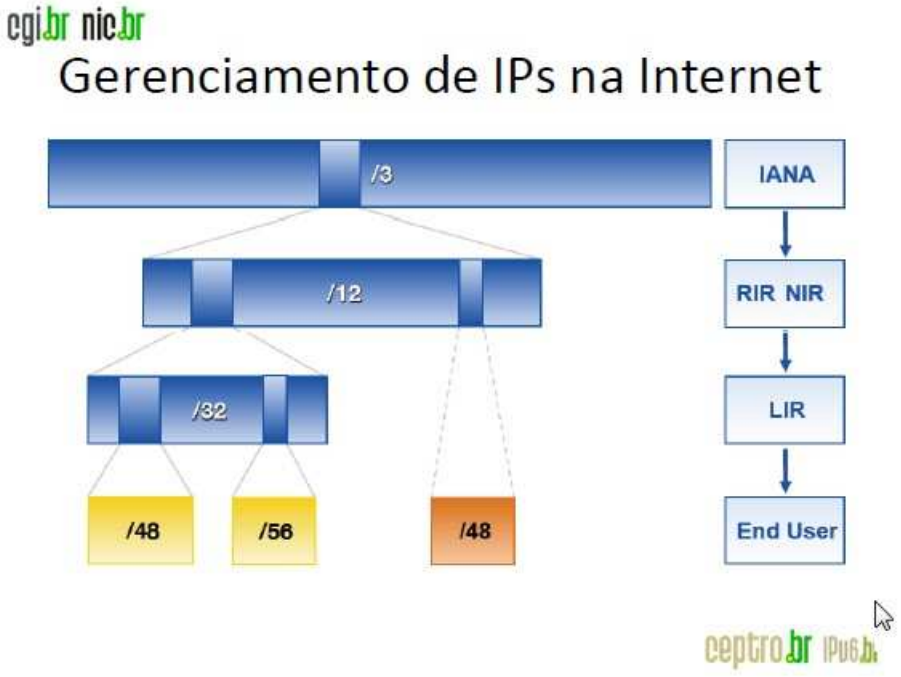


Figura 7 - Política de Designação de endereços da IANA

Para ajudar a gerenciar a distribuição dos 281.474.976.710.656 de endereços se faz necessário utilizar alguma ferramenta de registro e controle de utilização de endereços, que no caso foi adotado o IPPlan v6 (*IP Address Management Plan*) apresentado na figura 8.

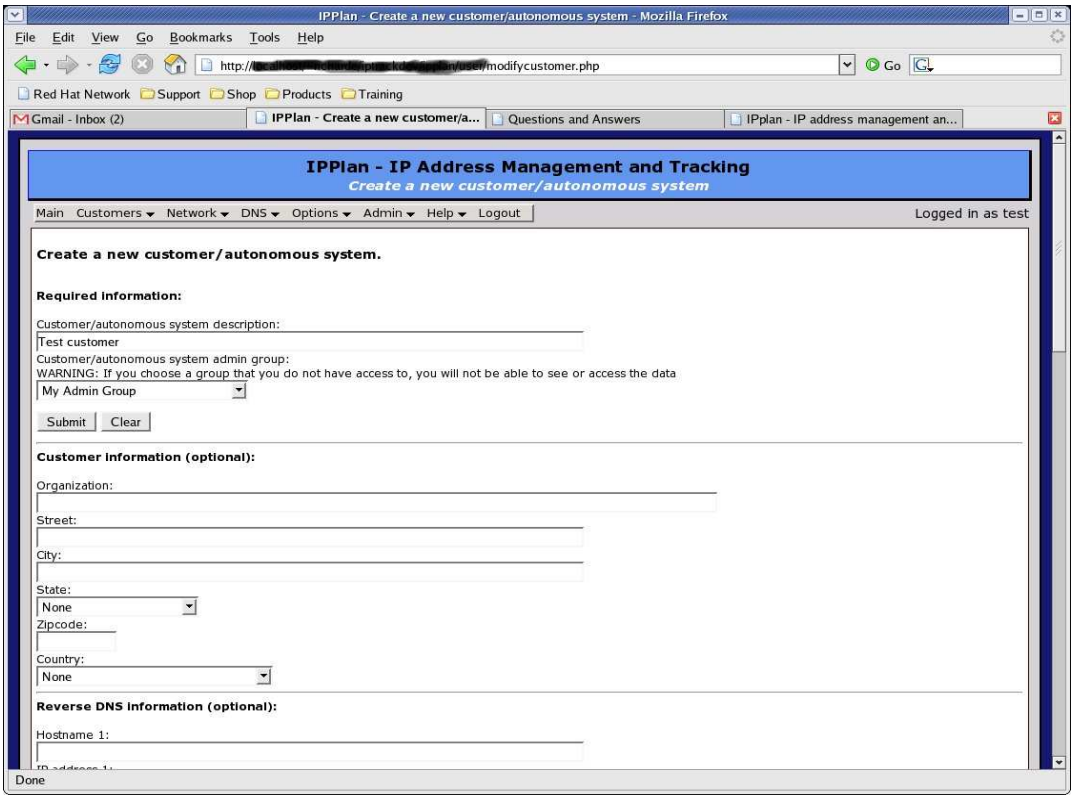


Figura 8 - Software de Controle de Distribuição de Endereços IP

5 **INTRODUÇÃO ÀS TÉCNICAS DE TRANSIÇÃO**

Neste capítulo serão analisadas as formas ou possibilidades para migração do protocolo IPv4 para o IPv6 e para tanto alguns questionamentos precisam ser respondidos:

1) A equipe envolvida possui habilidades ou conhecimentos suficientes para desempenho das atividades?
2) Os equipamentos e sistemas existentes são compatíveis ao novo protocolo?
3) É possível escolher uma data para a migração completa de toda infraestrutura?
4) Há necessidade que justifique o investimento?

Em resposta aos citados questionamentos que precisam ser feitos para um harmonioso plano de migração conclui-se que:

1) Havia necessidade de aperfeiçoamento de pessoal, o que foi sanado matriculando alguns no Curso Básico de IPv6 do NIC.br;
2) Após levantamento e analise de toda infraestrutura ficou constatado haver equipamentos e aplicações que precisavam sofrer atualizações para adequação ao novo protocolo;
3) Não seria possível de uma hora para outra migrar toda a rede para trabalhar exclusivamente com protocolo IPv6, pois são muitos equipamentos e aplicações envolvidas, além de que a curva evolutiva de instituições adeptas ao IPv6 está muito lenta, principalmente devido às operadoras prestadoras de serviço de dados ainda não estarem oferecendo serviços com tal tecnologia e nem possuírem previsão para fornecê-lo;

4) Como já foi mencionado no capítulo 1 a Internet com o protocolo corrente (IPv4) não possui mais possibilidade de crescimento, portanto a evolução se justifica plenamente para uma instituição de ensino e pesquisa.

Passou-se então a estudar a melhor técnica de utilização do IPv6 diante dos cenários descritos.

5.1 MECANISMOS DE TRANSIÇÃO

Com o objetivo de facilitar o processo de transição entre as versões do Protocolo Internet, algumas técnicas foram elaboradas para que todas as redes em IPv4 permaneçam compatíveis com o IPv6 havendo inicialmente a coexistência entre os dois protocolos, o que torna essencial para o sucesso da transição.

Os mecanismos de transição podem ser classificados nas seguintes categorias:

- Pilha Dupla: que provê o suporte a ambos os protocolos no mesmo dispositivo;
- Tunelamento: que permite o tráfego de pacotes IPv6 sobre estruturas de rede IPv4; e
- Tradução: que permite a comunicação entre nós com suporte apenas IPv6 com nós que suportam apenas IPv4;

Uma grande dificuldade na implantação do IPv6 é a diversificada variedade de técnicas de transição, prejudicando a escolha adequada de qual utilizar. A figura 9 exemplifica essa variedade de técnicas sendo empregadas segundo seu método de funcionamento.

Recomenda-se, de uma forma geral a utilização de alguns critérios na escolha da técnica a ser empregada [11], como:

- Deve-se dar preferência a técnicas que proporcionem a utilização de IPv6 nativo no usuário final;
- Deve-se dar preferência a técnicas *stateless (*sem necessidade de guardar informações, cada pacote é tratado de forma independente) ao invés de técnicas *statefull (com* necessidade de manter tabelas de estado com informações sobre os endereços ou pacotes para processá-los)*;*
- Deve-se evitar técnicas paliativas de prolongamento do IPv4 sem a implantação em paralelo do IPv6;
- Deve-se estudar a técnica mais adequada à topologia da rede a ser aplicada;
- Deve-se observar o grau de maturidade da técnica a ser empregada analisando, por exemplo, se há o suporte da mesma nos equipamentos e softwares utilizados.

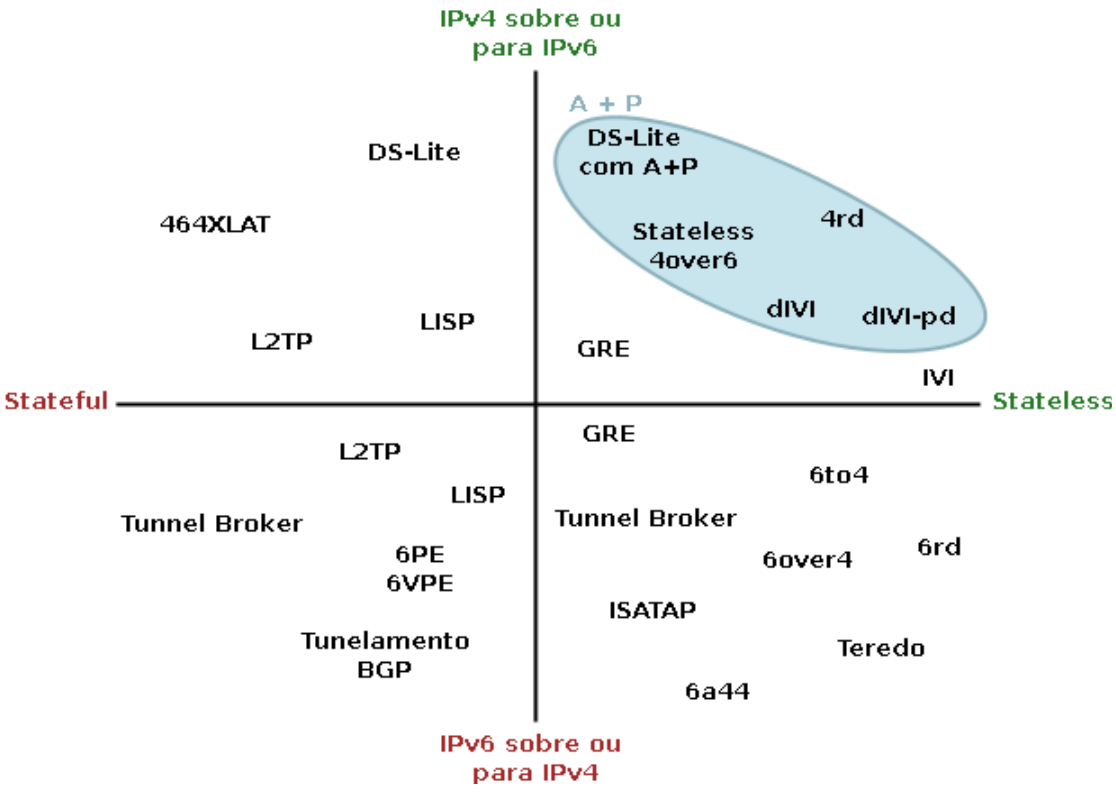


Figura 9 – Classificação das Técnicas de Transição

5.1.1 **Pilha Dupla**

A utilização desta técnica possibilita computadores e roteadores de estarem configurados com ambas as pilhas de protocolos, possuindo capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6. Sendo desta forma um nó IPv6/IPv4 ou nó Pilha Dupla, se comportando como um nó IPv6 quando se comunica com outro nó Ipv6, igualmente se comportará como um nó IPv4 quando se comunicar com outro nó IPv4.

Todo nó IPv6/IPv4 deve ser configurado com os dois endereços, utilizando seus respectivos mecanismos. O IPv4 através do DHCP ou configuração manual, por exemplo, para receber seu endereço IPv4, e o IPv6 através da configuração manual, autoconfiguração *stateless* e/ou DHCPv6 para também possuir seu respectivo endereço IPv6.

Esta técnica de transição permite uma implantação gradual, configurando pequenas áreas ou segmentos da rede de cada vez. Outra grande vantagem é que se algum dia o IPv4 deixar de ser utilizado basta desligá-lo na sua respectiva pilha. Na figura 10 é possível observar o funcionamento da pilha dupla.

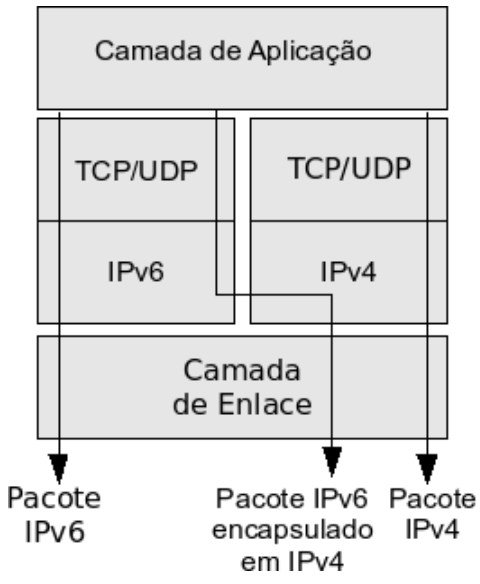


Figura 10 – Funcionamento da Pilha Dupla

5.1.2 **Técnicas de Tunelamento**

A técnica de criação de túneis permite enviar pacotes IPv6 através da já existente infraestrutura IPv4 sem realizar nenhuma mudança no roteamento, encapsulando todo o conteúdo do pacote IPv6 dentro de um pacote IPv4.

As técnicas de tunelamento têm sido muito utilizadas na fase inicial de implantação do IPv6 por serem de fácil aplicação e por ainda não existir facilmente oferta comercial de tráfego IPv6 nativo.

Existem muitas técnicas de tunelamento disponíveis. As suas dificuldades de implantação e diferença de desempenho mudam consideravelmente de um modelo para o outro de acordo com os cenários de uso, o que necessitaria um estudo detalhado de cada um. Dentre as diversas técnicas de tunelamento destacam-se as seguintes:

- Tunel Broker;
- 6to4;
- ISATAP;
- Teredo; e
- GRE.

Dentre os mencionados serão analisados apenas alguns para não fugir ao escopo do trabalho.

5.1.2.1 *Tunnel Broker*

Esta técnica tem a finalidade de prover o acesso de *hosts* IPv6/IPv4 em uma rede exclusivamente IPv4 à redes IPv6. Funciona basicamente através de conexão a um provedor de acesso de *Tunnell Broker,* que geralmente exige cadastramento prévio e instalação de *software* ou execução de *script* de configuração.

A conexão do túnel é realizada através da solicitação do serviço ao Servidor Web do provedor, que após autenticação, verifica qual tipo de conexão o cliente está utilizando (IPv4 público ou NAT) e lhe atribui um endereço IPv6. A partir daí o cliente pode acessar qualquer *host* IPv6 na Internet. Os *Tunnel Brokers* geralmente oferecem blocos fixos IPv6 que variam de /64 a /48.

Dentre as opções existentes se destacam a *Hurricane Eletric*, que provê túneis para usuários domésticos ou corporativos, inclusive com a possibilidade de se fechar sessões BGP para provimento de trânsito IPv6 via túnel, e a SixXS, que é mantida de forma colaborativa por intermédio de um grande número de organizações. Não é possível fechar conexões BGP, mas é possível obter redes fixas de tamanho /48 roteadas através do túnel. Na figura 11 é possível observar a topologia lógica do túnel *Broker.*

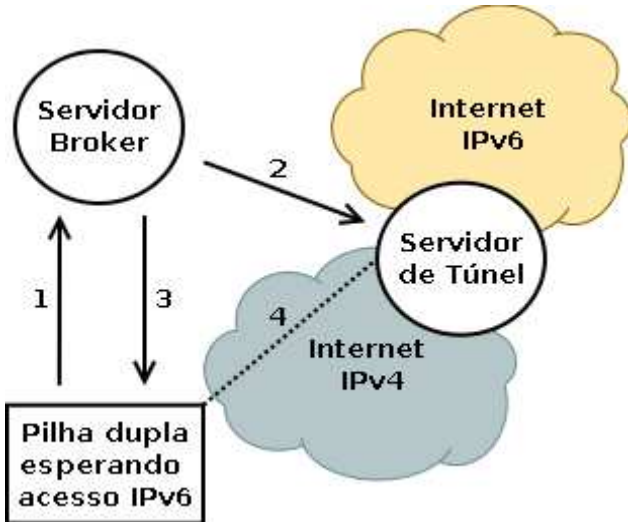


Figura 11 – Topologia Lógica do Túnel Broker

Na figura 11:

1 - Cliente pilha dupla solicita túnel (pode ser solicitada autenticação) via IPv4

2 - Broker cadastra usuário no Servidor de túnel

3 - Broker informa cliente parâmetros para criação do túnel

4 - Tunel estabelecido.

5.1.2.2 Teredo

A técnica de tunelamento automática Teredo foi criada pela Microsoft e definida na RFC 4380, permitindo que nós localizados atrás de *Network Address Translations* (NAT) possam obter conectividade IPv6 utilizando tunelamento IPv4, através do protocolo UDP.

A utilização do Teredo não é recomendada por ter se mostrado pouco eficiente com altas taxas de falhas e algumas considerações de segurança.

Existem dois personagens importantes no Teredo, o Servidor Teredo e o *Reply* Teredo. A conexão é realizada através do Servidor Teredo, que é iniciado logo após determinar que tipo de NAT está sendo utilizado na rede. Na sequência, caso o nó destino possua IPv6 nativo, um *Relay* Teredo é utilizado então para criar uma interface entre o cliente e o nó de destino. O *Relay* a ser utilizado sempre será o mais próximo do nó destino e não o mais próximo do cliente.

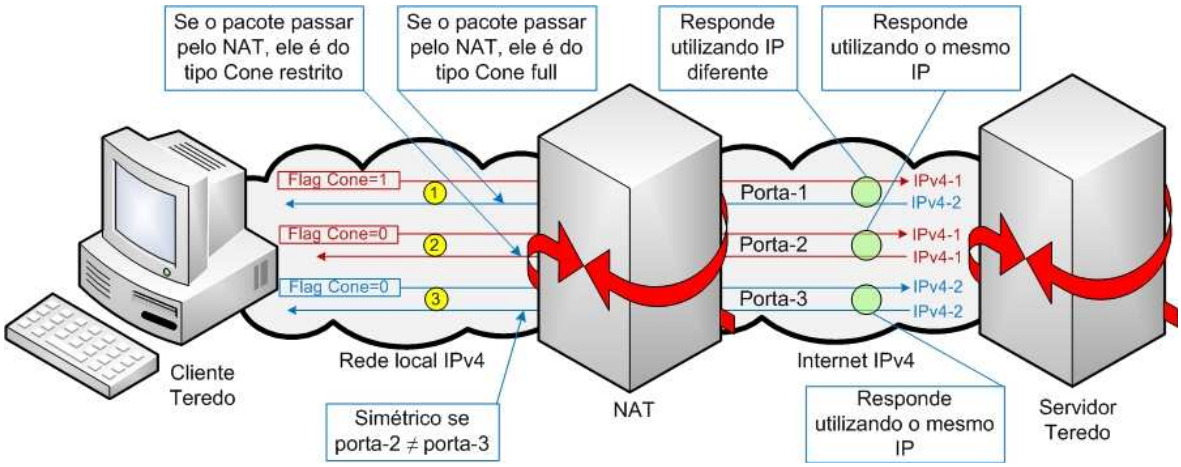


Figura 12 – Túnel Teredo

Na figura 12:

1- Uma mensagem *Router Solicitation* (RS) é enviada ao servidor Teredo 1 (servidor primário) com o *flag* de NAT tipo Cone ativado. O servidor Teredo 1 então responde com uma mensagem de *Router Advertisement* (RA). Como a mensagem

RS estava com o Cone *flag* ativado, o servidor Teredo 1 envia a mensagem RA utilizando um endereço IPv4 alternativo. Com isso o cliente conseguirá determinar se o NAT que ele está utilizando é do tipo Cone se ele receber a mensagem de RA;

2- Se a mensagem RA do passo anterior não for recebida o cliente Teredo envia uma outra mensagem RS, mas, agora com o Cone *flag* desativado. O servidor Teredo 1 responde novamente com uma mensagem RA, mas, como o Cone *flag* da mensagem RS estava desativado, ele responde utilizando o mesmo endereço IPv4 em que ele recebeu a mensagem RS. Se agora o cliente receber a mensagem de RA, então ele conclui que está utilizando NAT do tipo restrito;

3- Para ter certeza que o cliente Teredo não está utilizando um NAT do tipo simétrico, ele envia mais uma mensagem RS, mas, agora para o servidor secundário Teredo 2, o qual responde com uma mensagem do tipo RA. Quando o cliente recebe a mensagem RA do servidor Teredo 2, ele compara o endereço e a porta UDP de origem contidos na mensagem RA recebidas dos dois servidores. Se forem diferentes o cliente conclui que está utilizando NAT do tipo simétrico, o qual não é compatível com o Teredo.

Exemplo de configuração do um Linux como cliente Teredo:

Editar o arquivo de configuração do miredo:

 # vim /usr/local/etc/miredo/miredo.conf

Especifique o nome ou IP do servidor que você irá utilizar, você pode utilizar até 2 servidores, sendo que o primeiro é especificado pela entrada “ServerAddress” e o segundo por “ServerAddress2” seguida do IP ou nome do servidor:

```
#! /usr/local/sbin/miredo -f -c
# Nome da interface utilizada no tunel.
InterfaceName teredo
#Dependendo das regras do seu firewall/NAT ou tipo de NAT,
#voce precisa fixar a porta e o endereco IP a ser utilizado
#BindPort 3545
#BindAddress 192.0.2.100
#Servidores Teredo a serem utilizados(o maximo é 2)
ServerAddress teredo-debian.remlab.net
ServerAddress2 teredo.ipv6.microsoft.com
```

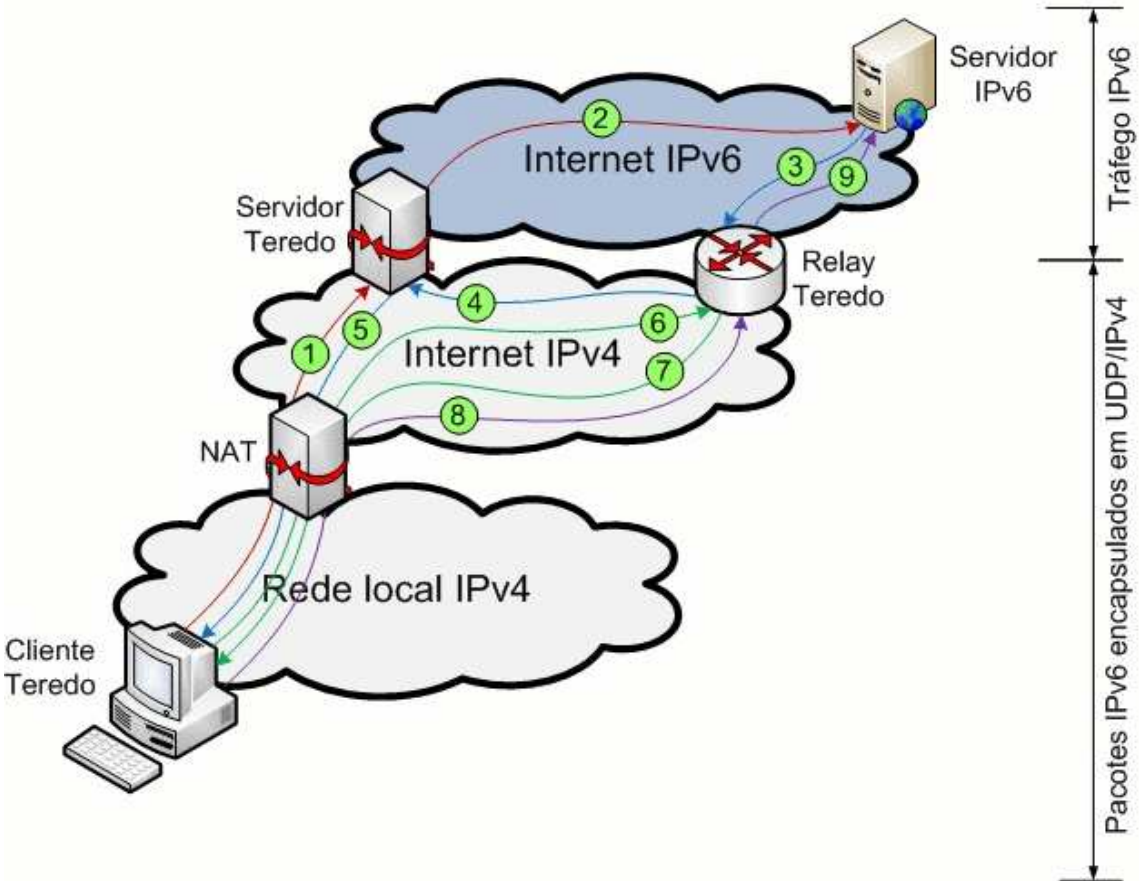


Figura 13 – Comunicação através de NAT restrito

Na figura13:

1- Para iniciar a comunicação, primeiro o cliente Teredo tem que determinar o endereço IPv4 e a porta UDP do *Relay* Teredo que estiver mais próximo do *host* IPv6, para isto, ele envia uma mensagem ICMPv6 *echo request* para o *host* IPv6 via o seu servidor Teredo;

2- O servidor Teredo recebe a mensagem ICMPv6 *echo request* e a encaminha para o *host* IPv6 através da rede IPv6;

3- O *host* IPv6 responde ao cliente Teredo com uma mensagem ICMPv6 *Echo Reply* que é roteada através do *Relay* Teredo mais próximo dele;

4- Através do pacote recebido, o *Relay* Teredo descobre que o cliente Teredo está utilizando um NAT do tipo restrito, sendo assim, se o *Relay* Teredo enviar o pacote ICMPv6 diretamente para o cliente Teredo, ele será descartado pelo NAT porque não há mapeamento pré-definido para tráfego entre o cliente e o *Relay*

Teredo. Com isso o *Relay* Teredo envia um pacote “*Bubble*” para o cliente Teredo através do Servidor Teredo utilizando a rede IPv4;

5- O servidor Teredo recebe o pacote “*Bubble*” do *Relay* Teredo e o encaminha para o cliente Teredo, mas coloca no indicador de origem o IPv4 e a porta UDP do *Relay* Teredo. Como já havia um mapeamento de tráfego entre o servidor Teredo e o Cliente Teredo, o pacote passa pelo NAT e é entregue ao Cliente Teredo;

6- O Cliente Teredo extrai do pacote “*Bubble*” recebido o IPv4 e a porta UDP do *Relay* Teredo mais próximo do *host* IPv6. Com isso, o Cliente Teredo envia um pacote “*Bubble*” para o *Relay* Teredo para que seja criado um mapeamento de conexão entre eles no NAT;

7- Baseado no conteúdo do pacote “*Bubble*” recebido, o *Relay* Teredo consegue determinar que ele corresponde ao pacote ICMPv6 *Echo Reply* que está na fila para a transmissão e também que a passagem através do NAT restrito já está aberta. Sendo assim ele encaminha o pacote ICMPv6 *Echo Reply* para o cliente Teredo;

8- Depois de recebido o pacote ICMPv6, um pacote inicial é então enviado do Cliente Teredo para o *host* IPv6 através do *Relay* Teredo mais próximo dele;

9- O *relay* Teredo remove os cabeçalhos IPv4 e UDP do pacote e o encaminha através da rede IPv6 para o *host* IPv6. Após isto os pacotes subsequentes são enviados através do *Relay* Teredo.

5.1.2.3 6to4

Conforme previsto na RFC 3056, a técnica de tunelamento automática 6to4 proporciona a ligação ponto-a-ponto entre computadores, subredes ou roteadores IPv6 por meio da rede IPv4, servindo um endereço IPv6 único composto a partir de

endereços IPv4 públicos. Este endereço 6to4 foi convencionado para utilizar o prefixo de endereço global 2002:wwxx:yyzz::/48, em que o wwxx:yyzz é o próprio endereço IPv4 público do cliente convertido em hexadecimal. Na figura 14 é possível observar o mecanismo de comunicação de um cliente 6to4 com outro também 6to4 estando em redes distintas.

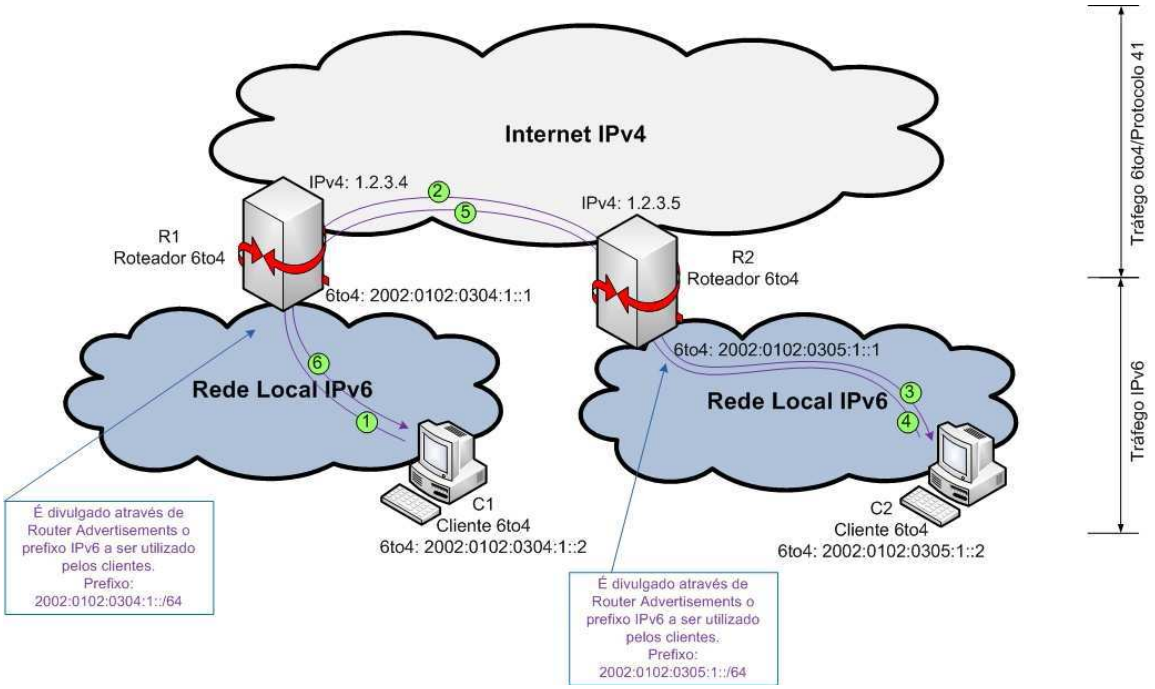


Figura 14 - Comunicação Cliente 6to4 com Cliente 6to4 em redes diferentes

É possível notar que o tráfego na rede local é nativo IPv6 e ele é encapsulado apenas entre os roteadores 6to4 conforme apresentado na tabela 1.

Tabela 1 - Tabela de Roteamento 6to4

Equipamento	Rota
C1	::/0 através de R1 2002:0102:0304:1::/64 através da interface LAN
R1	**::/0** através do Relay 6to4 utilizando a interface virtual 6to4 **2002::/16** através da interface virtual 6to4 **2002:0102:0304:1/64** para a rede local através da interface LAN
R2	**::/0** através de R2 **2002:0102:0305:1:/64** para a rede local através da interface LAN
C2	**::/0** através do *Relay* 6to4 utilizando a interface virtual 6to4 **2002::/16** através da interface Virtual 6to4 **2002:0102:0305:1:/64** para a rede local através da interface LAN

O prefixo do túnel 6to4 sempre será 2002, conforme definição da IANA, seguido do próximo campo que é o IPv4 público do cliente convertido em hexadecimal.

Alguns problemas de segurança no túnel 6to4 devem ser observados ao se planejar utilizá-lo [12]:

- O *Relay* roteador não verifica os pacotes IPv6 que estão encapsulados em IPv4, apesar dele os encapsular e desencapsular;

- O *spoofing* de endereço é um problema grave em túneis 6to4, podendo ser facilmente explorado;

- Não há um sistema de autenticação entre o roteador e o *Relay* roteador, facilitando assim a exploração de segurança através da utilização de *Relays* roteadores falsos.

Exemplo de configuração de Cliente/Roteador 6to4:

- Instale o suporte ao IPv6:
 # modprobe ipv6
- Ative o roteamento IPv6, editando o arquivo /etc/sysctl.conf e adicionando a seguinte linha:
net.ipv6.conf.default.forwarding=1
- Converta o endereço IPv4 para Ipv6/6to4 utilizando o seguinte comando:
Exemplo de conversão do IPv4 207.192.20.30 para 6to4:
 # printf "2002:%02x%02x:%02x%02x::1\n" 207 192 20 30

No caso do Debian e Ubuntu, edite o arquivo /etc/network/interfaces e acrescente a interface 6to4 conforme o seguinte exemplo:

auto sit0
iface sit0 inet6 static
address 2002:c000:0203::1 # IPv4 convertido para 6to4
netmask 16
gateway ::192.88.99.1 # endereço do relay a ser utilizado

- Nos outros casos você pode utilizar um script para ativar o túnel 6to4, sendo assim, faça o download do script utilizando o seguinte comando:
 # wget -c http://sites.inka.de/bigred/sw/6to4
Se você não for utilizar o relay padrão que é obtido via anycast (192.88.99.1), você terá que alterar duas variáveis no script:
REMOTE4=<IPv4 do Relay>
REMOTE6=<IPv6 6to4 do Relay>

Com tudo configurado, você já poderá iniciar o tunel 6to4 executando o seguinte comando:

 # ./6to4 up <IPv4 da Interface ligada à Internet> <interface ligada à sua rede local>

Exemplo: # ./6to4 up 200.192.170.10 eth0

Para desativar o túnel, você executa o seguinte comando:

 # 6to4 down <IPv4 da Interface ligada à Internet> <interface ligada à sua rede local>

Exemplo: # 6to4 down 200.192.170.10 eth0

Exemplo de configuração de Roteador Linux 6to4:

- Instale o suporte ao IPv6:

 # modprobe ipv6

- Ative o roteamento IPv6, editando o arquivo /etc/sysctl.conf e adicionando a seguinte linha:

net.ipv6.conf.default.forwarding=1

- Faça o download do script de configuração em utilizando o seguinte comando:

 # wget -c http://sites.inka.de/bigred/sw/6to4

- Se você for utilizar um relay diferente do padrão 192.88.99.1, é necessário que você modifique o a configuração do script de inicialização do roteador 6to4. Para configurá-lo, você precisará converter o endereço do relay para o formato do 6to4, para isto, utilize o seguinte comando:

Exemplo de conversão do IPv4 207.192.20.30 para 6to4:

printf "2002:%02x%02x:%02x%02x::\n" 207 192 20 30

Depois disso, edite o script e altere as seguintes variáveis:

REMOTE4=<IPv4 do Relay>

REMOTE6=<IPv6 6to4 do Relay>

- Instale o serviço de router advertisement: Para o Debian e Ubuntu utilize o seguinte comando:

 # apt-get install radvd

- Configure o Radvd editando ou criando o arquivo /etc/radvd.conf com o seguinte conteúdo:

```
interface eth0 { # ajuste de acordo com a interface conectada a sua rede local
AdvSendAdvert on;
MinRtrAdvInterval 20;
MaxRtrAdvInterval 60;
AdvLinkMTU 1400; # ajuste de acordo com suas necessidades
prefix 2002::/64 {
AdvOnLink off;
AdvAutonomous on;n
AdvRouterAddr on;
Base6to4Interface tun64;
AdvPreferredLifetime 90;
AdvValidLifetime 120;
};
};
```

- Com tudo configurado, você já poderá iniciar o seu roteador executando o seguinte comando:

 # 6to4 up <IPv4 da Interface ligada à Internet> <interface ligada à sua rede local>

Exemplo:

6to4 up 200.192.170.10 eth0

- Para testar se o roteador 6to4 está com conectividade à rede IPv6, execute o seguinte comando:

 # traceroute6 ipv6.google.com

ou se o DNS não estiver resolvendo IPv6

 # traceroute6 2001:4860:0:2001::68

- Para testar se o roteador esta funcionando corretamente, coloque um computador com suporte a IPv6 na rede local e execute novamente o comando acima, ela deverá pegar automaticamente um IPv6 6to4 conforme o prefixo anunciado pelo Radvd.

Exemplo de configuração no Windows:

- Windows Vista já ativa automaticamente o cliente 6to4 quando ele possui endereço Ipv4 Público.
- Windows XP e Windows 2003:
- Primeiro faça todas as atualizações via Windows Update;
- Ative o suporte ao IPv6 executando o seguinte comando:

> netsh int ipv6 install

- Ative e configure o 6to4 executando o seguinte comando:

> netsh int ipv6 6to4 set relay <IPv4 do relay> enabled <MTU>

Exemplo utilizando o relay padrão anycast:

> netsh int ipv6 6to4 set relay 192.88.99.1 enabled 1440

5.1.3 **Técnicas de Tradução**

A tradução é uma técnica que possibilita a comunicação entre nós que suportam apenas um padrão de protocolo IP. Essa técnica é empregada de diversas formas e em camadas distintas, traduzindo cabeçalhos de IPv4 para IPv6 e vice-versa, realizando as devidas conversões de endereços e trabalhando com pacotes TCP ou UDP.

Dentre as diversas técnicas de tradução podem ser mencionadas as seguintes: SIIT (*Stateless IP/ICMP Translation*), BIS (*Bump-in-the-Stack),* BIA *(Bump in the API*), TRT (*Transport Relay Translator*), ALG (*Application Layer Gateway*) e DNS-ALG (*DNS Application Layer Gateway*). Porém, nenhuma delas merece destaque porque praticamente todos os *hosts* que suportam conexão IPv6

também suportam IPv4, e as técnicas de tradução implicam em problemas relacionados a incompatibilidade com alguns mecanismos de segurança existentes, similarmente ao que ocorre com o NAT no IPv4, havendo assim técnicas mais eficientes do que as de tradução.

6 **CONFIGURAÇÕES**

Foi utilizado para o projeto uma Máquina Virtual com 2 processadores de 2.8 GHz, 2GB de memória RAM e Disco Rígido de 80 GB, rodando o Sistema Operacional Linux Ubuntu 12.04.02 LTS com kernel 3.5.0-23-generic, arquitetura x86_64 (64bits)

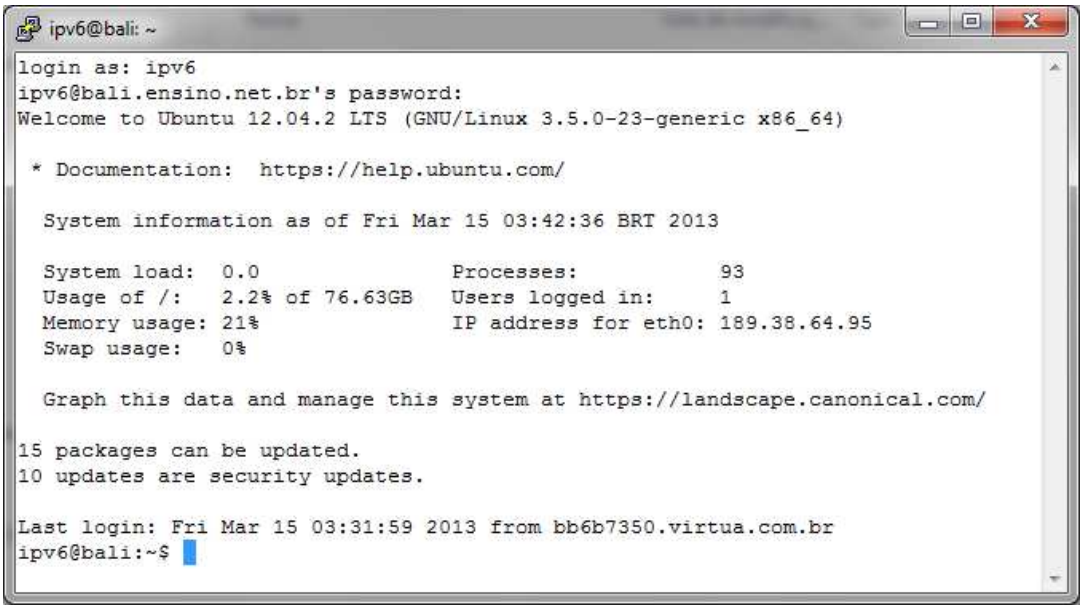


Figura 15 - Máquina Virtual para Testes

6.1 CONFIGURAÇÃO DE UMA INTERFACE ETHERNET

A maioria dos Sistemas Operacionais atualmente já vêm habilitados para operar com IPv6, porém ao se iniciar o projeto de implantação do IPv6 no DECEx foi necessário entender o funcionamento dos módulos que são carregados no kernel do Linux, e logo foi percebido a necessidade de habilitar o módulo do IPv6:

A interface de rede no Linux deve ser configurada editando-se o arquivo interfaces que fica localizado em: */etc/network/interfaces.*

Através do comando *ipv6@bali:~$ vim /etc/network/interfaces* é possível editar o arquivo de configuração das interfaces de rede conforme se pode observar na figura 16.

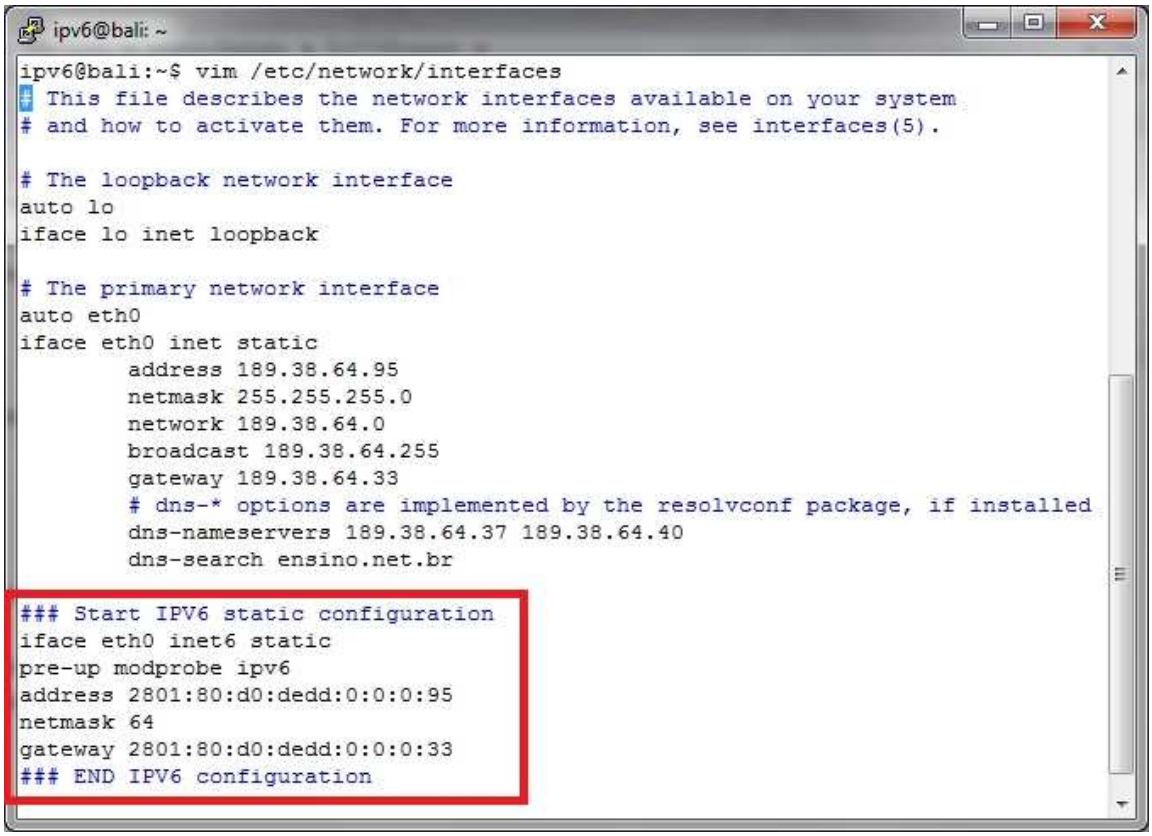


Figura 16 - Arquivo de Configuração das Interfaces de Rede

Após a configuração do arquivo /etc/interfaces deve-se executar o comando *ifconfig* obtendo o resultado exibido na figura 17, onde é possível observar a pilha dupla: IPv4 e IPv6 configurados na mesma interface.

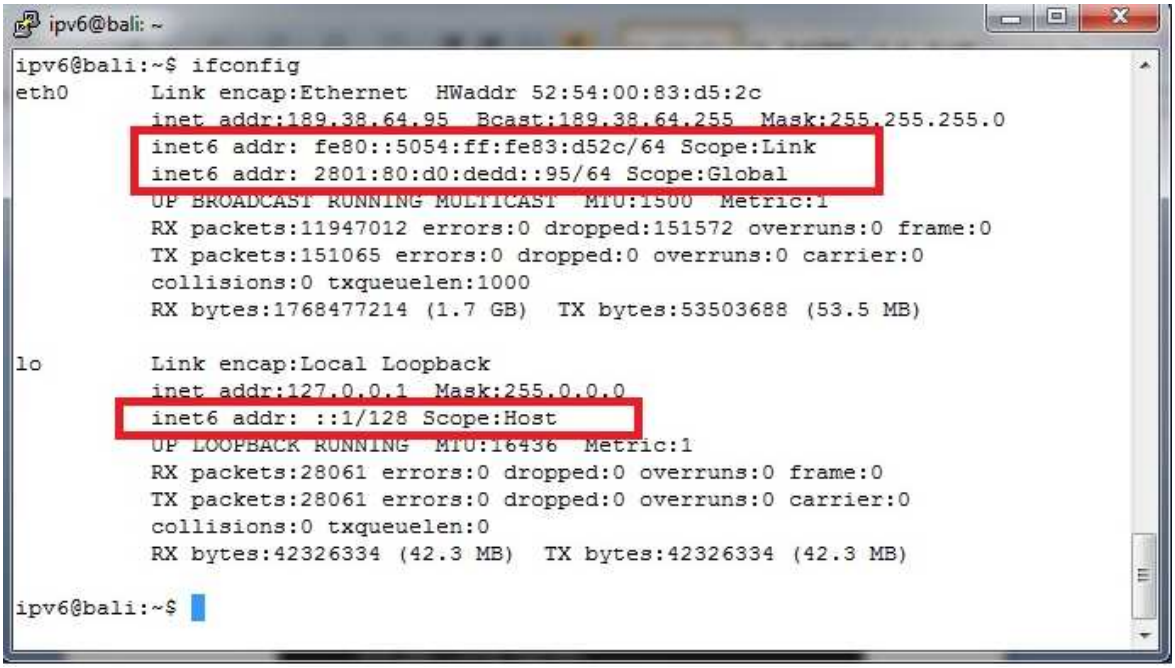


Figura 17 - Comando IFCONFIG

6.2 SISTEMA DE NOMES PARA IPV6

O DNS (*Domain Name System*) é um serviço que torna o acesso a Internet amigável, facilitando seu uso através do mapeamento de nomes (Endereços dos sites) em endereço IP, de forma transparente para o usuário final.

Segundo Kurose e Ross (2010) [2] o DNS é um banco de dados distribuído implementado em uma hierarquia de servidores de nome (servidores DNS), e um protocolo de camada de aplicação (UDP 53) que permite que hospedeiros consultem o banco de dados distribuído.

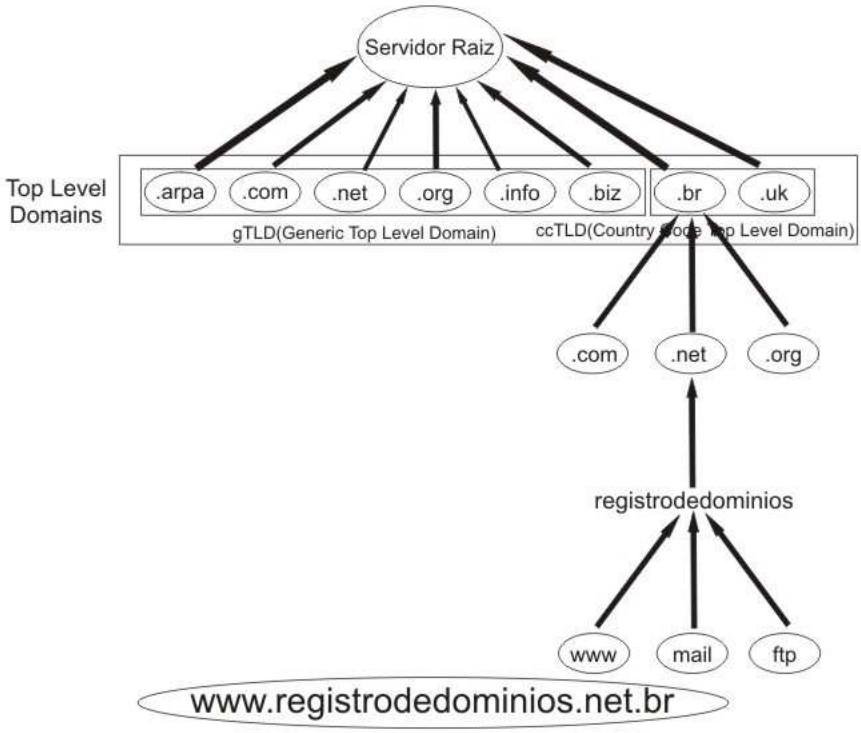


Figura 18 – Hierarquia dos domínios de Internet

Na prática quando um usuário requisita um endereço de Internet, como por exemplo: www.nce.ufrj.br, o servidor de nomes que recebeu o pedido repassa-o para o servidor responsável, e esse retorna para o requerente o endereço IP do host na forma de 32 bits. Para que o mesmo cenário descrito também funcione com IPv6, algumas alterações em sua configuração são necessárias, conforme prevê a RFC

1886 [13], para que um nome de domínio possa ser mapeado em um endereço de 128 bits. Resumidamente as alterações necessárias são as seguintes:

a) Criação de um novo tipo de registro chamado de AAAA, para mapear endereços de 128 bits;
b) Criação de um novo domínio (IP6.int), para permitir que endereços de hosts IPv6 possam inversamente encontrar o nome do domínio que responde por ele, semelhante com (.in.addr.arpa) do IPv4.

6.2.1 **Arquivos de Configuração**

Os servidores de nome são frequentemente máquinas UNIX que executam o software BIND (*Berkeley Internet Name Domain*). Sua configuração é feita através de alguns arquivos. O arquivo principal é o **/etc/named.conf** na versão BIND9. Este arquivo irá definir o diretório da base de dados do DNS e os parâmetros para definição dos domínios e sub-domínios (chamados *zones*). Para o BIND9 o padrão é **/var/named**.

No diretório definido estão os arquivos que descrevem os domínios. Estes arquivos são formados por registros de diversos tipos. Os principais registros estão descritos na Tabela 2:

Tabela 2 – Principais Registros de DNS

SOA	Start of Authority
NS	Name server
A	Name to address mapping
AAAA	Name to IPv6 address mapping
PTR	Address to name mapping
CNAME	Cannonical name (aliases)
TXT	Textual information
RP	Responsible person
MX	Mail exchange
HINFO	Host information
LOC	Location

Podem existir entradas de controle conforme apresentada na tabela 3.

Tabela 3 – Entradas de Controle do DNS

$ORIGIN subdomínio	Muda a origem do domínio para as definições subsequentes
$INCLUDE arq.zone	Inclui o arquivo arq.zone
$TTL tempo	Define o tempo de vida default em segundos. Podem ser utilizados os sufixos M, H, D, W para minutos, horas, dias ou semanas.

Comentários podem ser inseridos por '**;**'.

Exemplo de arquivo de configuração de um servidor DNS:

$ORIGIN com.br.

```
$TTL 1D
Exemplo         IN SOA exemplo.com.br. suporte.exemplo.com.br. (
                2007112201    ; serial
                43200         ; refresh
                3600          ; retry
                3600000       ; expiry
                86400         ; minimum
                    )
                IN TXT  "Dominio Virtual Exemplo"
                IN NS   ns.exemplo.com.br.
                IN A    189.107.115.80
                IN NS   ns.exemplo.com.br.
                IN NS   ns2.exemplo.com.br.
                IN MX   10 mail.examplo.com.br.
                IN RP   suport.exemplo.com.br.suport.exemplo.com.br.
                IN LOC  44 00 00.000 S 19 30 00.000 W 860.00m 0.00m
10000.00m 10.00m
$ORIGIN exemplo.com.br.
apollo          A           189.107.115.80
apollo          AAAA        2801:d0:dedd::80
atlas           A           189.107.115.81
atlas           AAAA        2801:d0:dedd::81
ftp             CNAME       atlas
mail            A           189.107.115.82
mail            AAAA        2801:d0:dedd::80
ns              CNAME       189.107.115.80
ns2             A           189.107.115.83
www             A           189.107.115.84
www             AAAA        2801:d0:dedd::84
```

Exemplo de trecho do arquivo de configuração do DNS reverso:

```
localhost       .       IN      A       127.0.0.1
```

```
1.0.0.127.in-addr.arpa.                 IN          PTR          localhost.
;
 localhost.                             IN          AAAA         ::1
;
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.int.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0         IN          PTR          localhost.
```

6.3 ROTEAMENTO IPv6

O recurso alocado pelo Registro.br aos ASs é um bloco IP que representa um grupo de endereços IP. O bloco não é um elemento roteável, o que é roteável é o prefixo. O que é possível, por exemplo, é criar um prefixo IPv6 /32 igual ao bloco /32 recebido do Registro.br e anunciar esse prefixo na tabela de rotas.

Cabe revisar algumas características básicas sobre o funcionamento dos mecanismos de roteamento, tanto interno (IGP) quanto externo (EGP), com foco nas principais mudanças em relação ao IPv6. Serão abordados os protocolos OSPF e BGP por serem os já empregados na instituição objeto do estudo.

6.3.1 **OSPFv3** (*Open Shortest Path First version 3)*

O OSPF é um protocolo do tipo *link-state* onde, através do processo de *flooding* (inundação), os roteadores enviam *Link State Advertisements* (LSA) informando seu estado atual ao SA. O *flooding* consiste no envio de um LSA por todas as interfaces de saída do roteador, de modo que todos os roteadores que receberem um LSA também o enviam por todas as suas interfaces. Com isso, o conjunto dos LSAs de todos os roteadores forma um banco de dados de estado do enlace, onde cada roteador participante do SA possui um banco de dados idêntico.

Com as informações desse banco, o roteador, através do protocolo OSPF, constrói um mapa da rede que será utilizado para determinar uma árvore de caminhos mais curtos dentro de toda a subrede, tendo o próprio nó como raiz. Ele utiliza o algorítimo de Dijkstra para a escolha do melhor caminho e permite agrupar os roteadores em áreas.

O OSPFv3 é um protocolo específico para IPv6, apesar de ter sido baseado na versão do OSPFv2, utilizada em redes IPv4. Deste modo, em uma rede com Pilha Dupla, é necessário utilizar OSPFv2 para o roteamento IPv4 e OSPFv3 para realizar o roteamento IPv6.

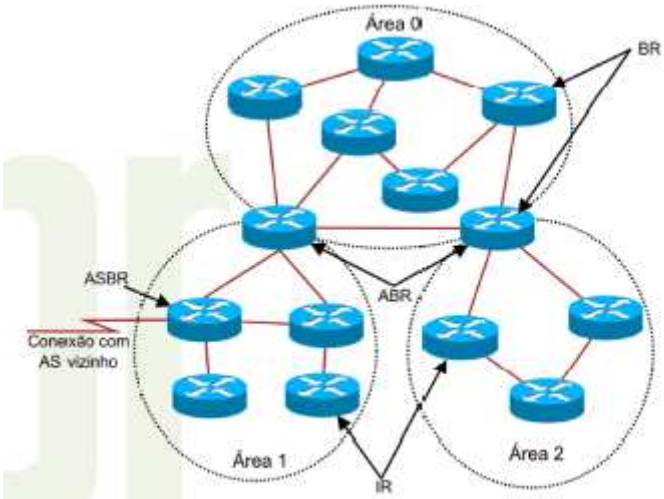


Figura 19 – Roteadores OSPF

Os roteadores OSPF podem ser classificados da seguinte forma, como exibe a figura 19:

• *Internal Router* (IR) – roteadores que se relacionam apenas com vizinhos OSPF de uma mesma área;

• *Area Border Router* (ABR) – roteadores que conectam uma ou mais áreas ao *backbone*.

• *Backbone Router* (BR) – roteadores pertencentes a área *backbone*. Um ABR é sempre um BR, desde que todas suas interfaces estejam diretamente conectadas ao *backbone* ou conectadas via *virtual link* - túnel que conecta uma área ao *backbone* passando através de outra área; e

• *Autonomous System Border Router* (ASBR) – roteadores que trocam informações de roteamento com roteadores de outro SA e distribuem as rotas recebidas ao longo do seu próprio SA.

Entre as principais diferenças entre o OSPFv2 e o OSPFv3 destacam-se:

• OSPFv3 roda por enlace e não mais por sub-rede

• Foram removidas as informações de endereçamento

• Adição de escopo para *flooding*

• Suporte explícito a múltipla instâncias por enlace

• Uso de endereços *link-local*

• Mudanças na autenticação

• Mudanças no formato do pacote

• Mudanças no formato do cabeçalho LSA

• Tratamento de tipos de LSA desconhecidos

• Suporte a áreas Stub/NSSA

• Identificação de vizinhos pelo Router IDs

• Utiliza endereços *multicast* (*AllSPFRouters* **FF02::5** e *AllDRouters* **FF02::6**)

6.3.2 BGP (*Border Gateway Protocol*)

As informações sobre as rotas da Internet encontram-se na tabela BGP. Em roteadores de borda, que tratam da comunicação entre SAs, essas informações são replicadas para a RIB e para a FIB, IPv4 e IPv6. A tabela global IPv4 possuiu hoje aproximadamente 300.000 entradas. A tabela IPv6 possui aproximadamente 2.500 entradas. A duplicidade dessas informações em arquiteturas distribuídas implica na necessidade de mais espaço para armazenamento, mais memória e mais processamento, tanto no módulo central quanto nas placas das interfaces.

Estes dados implicam em outro aspecto importante, a necessidade de se estabelecer um plano hierárquico de endereçamento para minimizar a tabela de rotas e otimizar o roteamento, evitando o anúncio de rotas desnecessárias e desagregadas. Na figura 20 é possível observar sessões BGP estabelecidas.

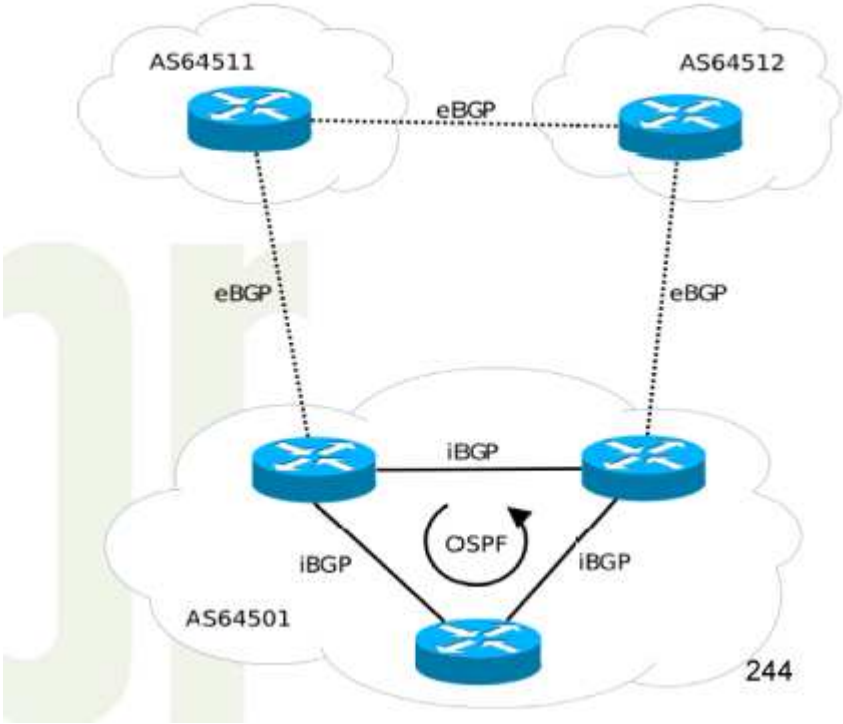


Figura 20 – Estabelecendo Sessões BGP

7 **TESTES DE VALIDAÇÃO**

Após as configurações realizadas no servidor web conforme apresentadas no capítulo 6, mais alguns pacotes e ferramentas foram instalados para as análises e testes. Foram instalados o Apache2, o PHP 5 e o MySQL 5 9 (figura 21) a fim de que fosse possível subir uma aplicação web. Como solução de conteúdo para o servidor web foram instalados os dois CMS´s (*Content Management Systems*): Joomla 3.0 e Wordpress 3.5, que podem neste instante ser acessados via IPv6 ou IPv4 nas seguintes URL´s respectivamente: http://bali.ensino.net.br/joomla ou http://bali.ensino.net.br/wordpress . Obedecendo o critério de pilha dupla, o cliente que tiver Ipv4 acessará os sites pelo IP 187.38.64.95 e o cliente que tiver Ipv6 nativo, via túnel ou por tradução, acessará os sites pelo seguinte endereço Ipv6: 2801:80:d0:d3dd::95.

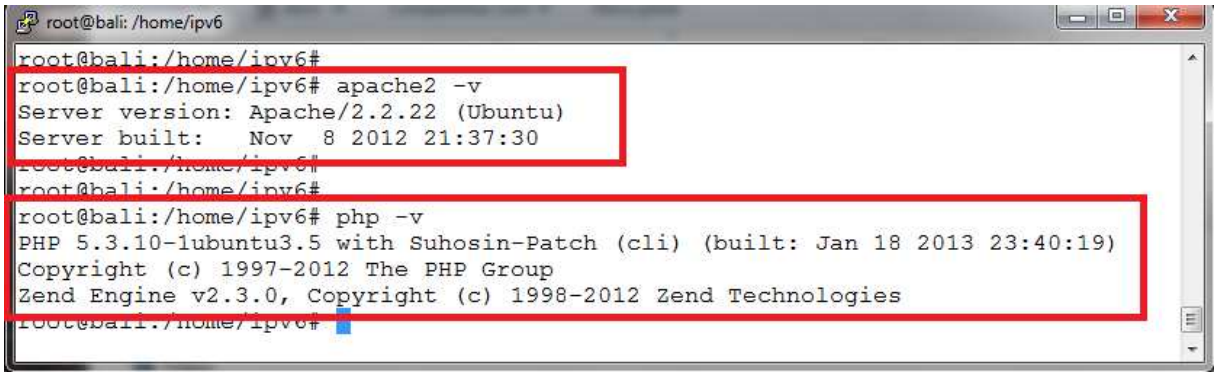


Figura 21 – Aplicações Instaladas

7.1 PING6

O comando *ping* é usado pelo protocolo ICMP que serve para testar a conectividade entre equipamentos e foi criado para uso em redes com a pilha de protocolo TCP/IP.

Para teste com a pilha IPv6 o comando precisa ser usado no Linux seguido do número 6, ficando ping6.

#ping6 –n –c 4 ietf.org

Este foi um comando executado na figura 22, onde o parâmetro –n serve para não resolver nomes e o parâmetro –c determina a quantidade de pacotes a serem enviados, no caso 4.

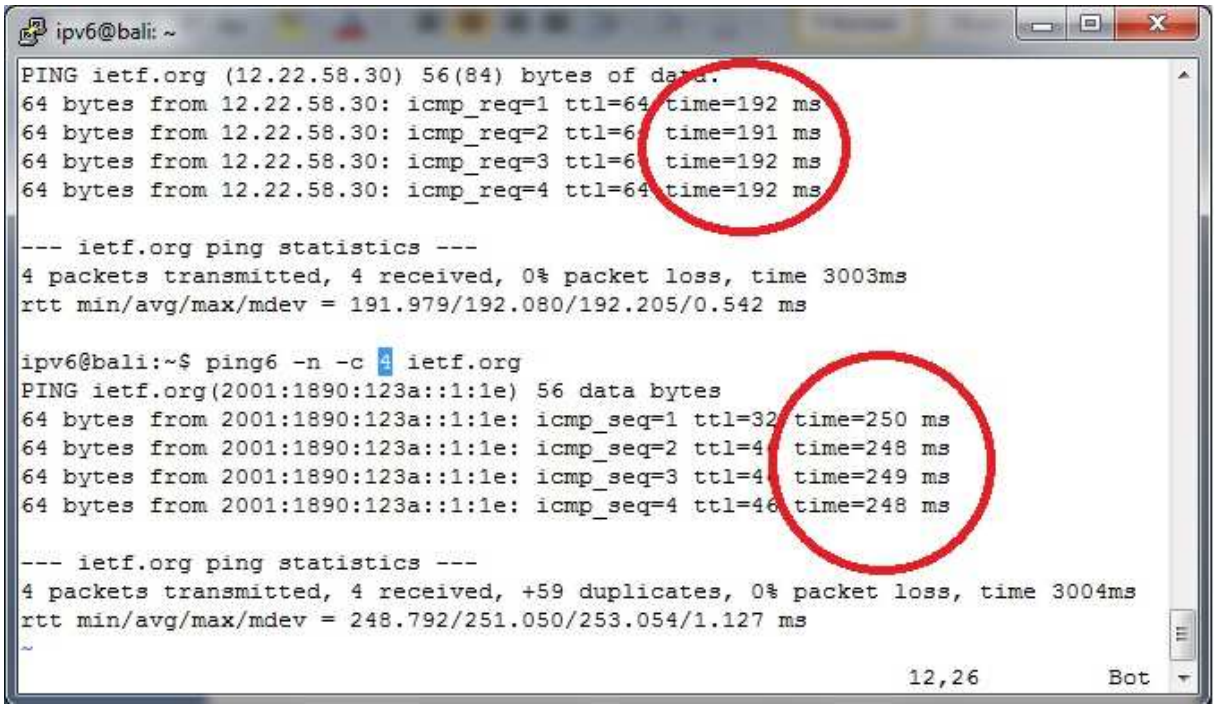


Figura 22 – Apresentação do Comando ping e ping6

7.2 MTR

O comando *mtr* pode ser empregado para analisar o estado de um enlace verificando possivelmente em que ponto do enlace existe algum problema. No teste demonstrado na figura 23 foi feito uma simulação de rota para o site do ipv6.br forçando a não resolução de nomes utilizando o parâmetro –n. O comando *mtr* serve para as duas pilhas sendo que ele dá preferência para sair em IPv6 quando este estiver ativado.

#mtr –n ipv6.br

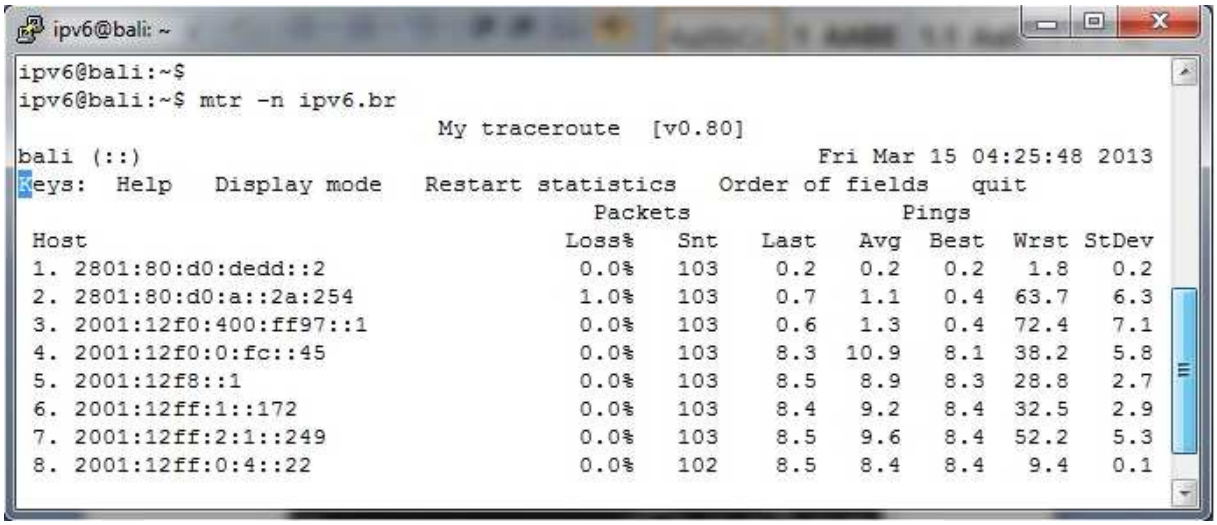


Figura 23 - Teste de rota exclusivamente IPv6

7.3 NETSTAT

O *netstat* é uma ferramenta, comum ao Windows, Unix e Linux, utilizada para se obter informações sobre as conexões de rede (de saída e de entrada), tabelas de roteamento, e uma gama de informações sobre as estatísticas da utilização da interface na rede.

Na figura 24 o comando *netstat* foi executado com os parâmetros -6 e –rn que serve para exibir a tabela de roteamento IPv6. É possível identificar a rota padrão através de ::/0.

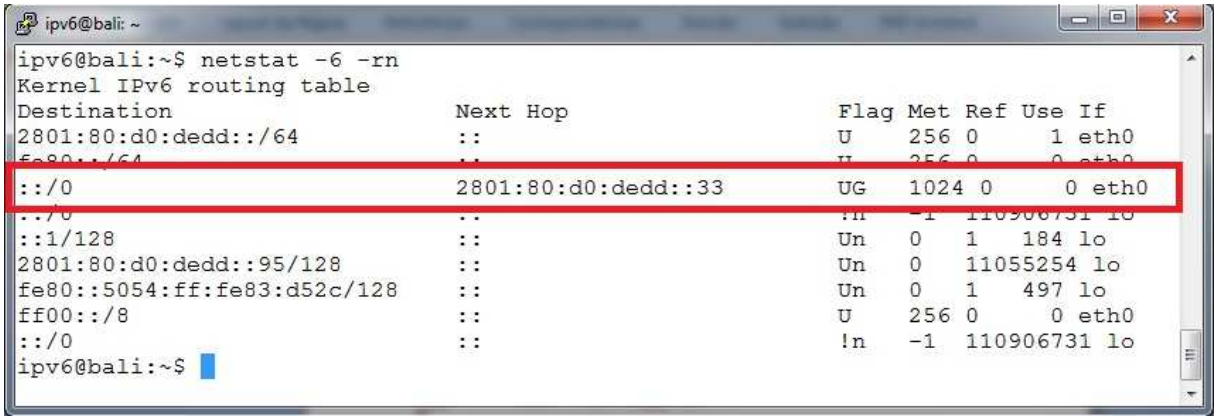


Figura 24 – Verificação de default Gateway

7.4 VALIDADOR DE SITES IPV6

O NIC.br possui um site chamado ipv6.br para ajudar a fomentar a implantação do IPv6 no Brasil. Dentre os diversos materiais e ferramentas disponibilizados no site existe um validador de servidores web no seguinte endereço: http://validador.ipv6.br/ . Basta digitar o endereço do seu servidor e mandar validar que a aplicação executará testes como os apresentados na figura 25, verificando se existe um endereço IPv6 atrelado àquela URL e com DNS Reverso configurado.

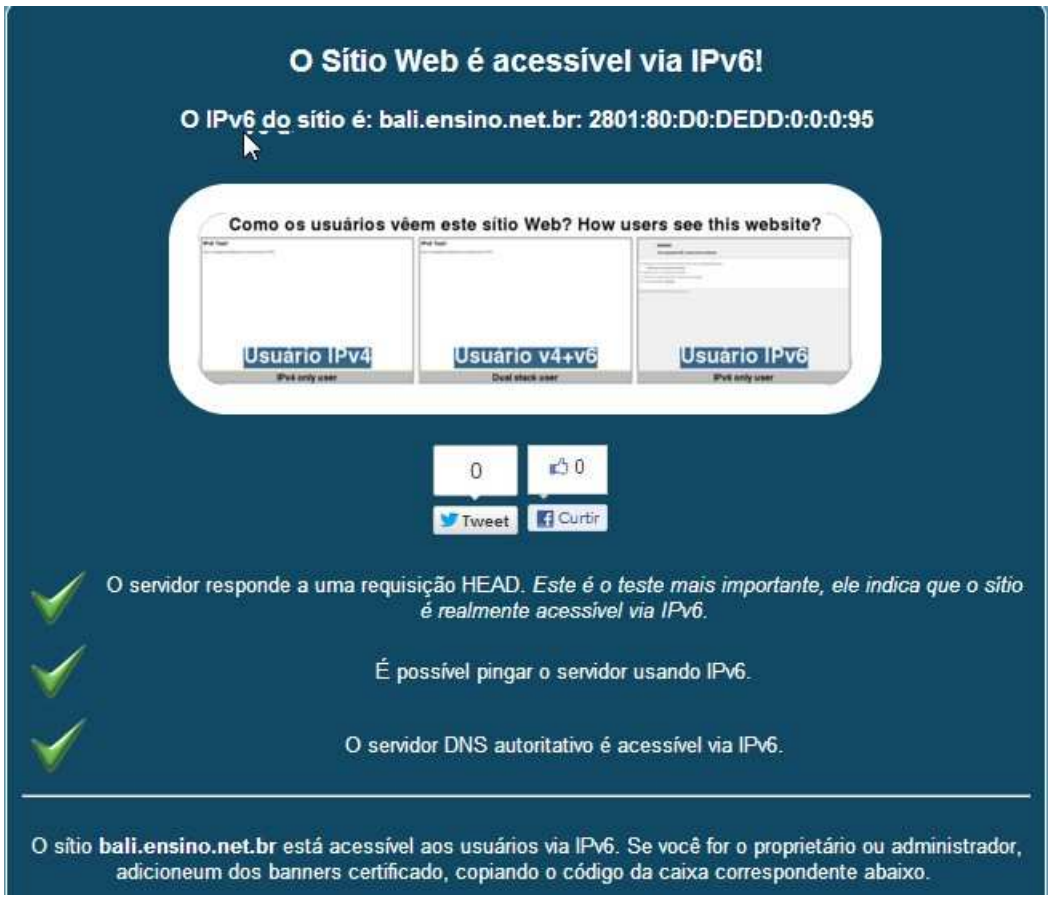


Figura 25 - Validação do Site IPv6

8 **CONCLUSÃO**

Após 30 anos de Internet os seres humanos têm analisado o quanto ela evolui, cresceu e tem deixado toda a sociedade cada vez mais dependente, seja pelas notícias em tempo real, seja pelo encurtamento de distâncias proporcionado pelas aplicações de videoconferêcia, mensagens instantâneas ou redes sociais.

Apesar de já ter ocorrido enorme crescimento e evolução como já mencionado, é sabido que a mente humana e seu poder criativo não têm limites, porém os recursos se esgotam e com a Internet no padrão atual não acontece diferente, seu poder de expansão está se exaurindo. Os endereços IPv4 estão se esgotando, o que de certa forma pode até soar positivo pois pode ser a oportunidade de se recomeçar. Começar novamente, porém com diversas lições aprendidas para sanar falhas e problemas que só vinham sendo remediados paliativamente e nunca curados. Problemas como visão limitada de crescimento, fragilidades de segurança, incapacidade de se adequar a uma multimídia de alta qualidade.

O IPv6 foi exaustivamente pensado para atender todas as limitações do IPv4, todavia com a sua praticidade e capacidade de comunicação que alavancaram a grande rede mundial de computadores.

Apesar do novo protocolo já estar pronto a algum tempo, poucos já ouviram falar sobre ele e menos ainda o utilizam. As prestadoras de serviço de dados ainda não têm previsão de quando estarão oferecendo o serviço comercialmente. Isso se deve claramente pela falta de interesse destas empresas pois acarretará investimentos que muitas vezes serão muito altos. Enquanto não é possível ter nativamente nas casas, alguns institutos de pesquisa e centros acadêmicos têm fomentado em suas cadeiras o conhecimento muitas vezes prático da tão esperada tecnologia.

O DECEx por se enquadrar nessa categoria mencionada (Centro de Educação e Pesquisa) não poderia ficar para trás e deixar de utilizar os melhorados recursos que já estão disponíveis.

Após o estudo do IPv6 e análise do cenário para emprego da nova tecnologia com todas as suas peculiaridades, conclui-se que é viável a implantação utilizando-se o modelo de Pilha Dupla para garantir a continuidade das aplicações e equipamentos que não suportam a nova tecnologia, assim como a elaboração de um plano de substituição destas aplicações e equipamentos por novos que possuam integramente a devida capacidade de operação.

Os testes demonstraram ser viável a operação com o modelo de transição adotado, apesar de ter sido notado um ligeira queda de desempenho da rede conforme observado na figura 22, onde pacotes ICMPv6 foram mais lentos que o ICMP, quando era esperado justamente o contrário.

A técnica adotada exige uma carga extra de trabalho e preocupação para os administradores de rede, uma vez que agora existem duas redes em paralelo, uma IPv4 e outra IPv6. Por Exemplo: um servidor que se queira colocar na web para disponibilizar um novo serviço deverá ser configurado para IPv4 e também para IPv6. Ele precisará ser cadastrado no DNS com seus dois registros A e AAAA e também constar nas regras de segurança do firewall tanto nas regras do IPv4 quanto no IPv6. Em contrapartida está livre das preocupações de *spoofing* e negação de serviço existentes nas técnicas de tunelamento.

Apesar do *overhead* inicial concluo ser perfeitamente viável a interoperabilidade entre os protocolos em Pilha Dupla.

REFERÊNCIAS

[1] Deering, S., Hinden, R., **“Internet Protocol – Version 6 (IPv6) Specification”, RFC 2460**, Dezembro 1998.

[2] KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet.** 5. Ed. São Paulo, 2010.

[3] FOROUZAN, BEHROUZ A.. **Comunicação de dados e redes de computadores**. 4. Ed. Porto Alegre: Bookman, 2007.

[4] FOROUZAN, BEHROUZ A.. **TCP/IP - Curso Completo** - 3ª Ed. Mac Graw Hill

[5] TANENBAUM, Andrew S. **Redes de Computadores**. 5. ed [s. l.]: Campus, 2003. Cap 5.Nsso

[6] SILVA, ADAILTON J. S. **Hierarquia de Endereços IPv6.** Disponível em: <http://www.rnp.br/newsgen/0103/end_ipv6.html#ng-1-1>. Acesso em mar. 2013.

[7] MPOG (Ministério do Planejamento, Orçamento e Gestão). **Opção pelo Software Livre.** Disponível em: <http://www.planejamento.gov.br/secretaria.asp?cat=75&sub=107&sec=7>. Acesso: mar. 2013.

[8] EB (Exército Brasileiro). **Educação e Cultura**. Disponível em: <http://www.exercito.gov.br/web/guest/educacao-e-cultura>. Acesso em mar. 2013.

[9] **DECEx** (Departamento de Educação e Cultura do Exército). . Disponível em: <www.decex.ensino.eb.br>. Acesso em mar. de 2013.

[10] NIC.br (Núcleo de Informação e Coordenação do ponto BR). **PTTMetro**. Disponível em: <http://ptt.br/intro> . Acesso em mar. 2013.

[11] NIC.br (Núcleo de Informação e Coordenação do ponto BR). **Apostila IPv6 Básico.** São Paulo 2012. Disponível em: <http://ipv6.br/download/ApostilaIPv62012.pdf>. Acesso em mar. 2013.

[12] NIC.br (Núcleo de Informação e Coordenação do ponto BR). **Curso IPv6 Básico**. São Paulo 2010 Disponível em: <http://ipv6.br/download/IPv6-apostila.pdf>. Acesso em mar 2013.

[13] THOMSON, S e HUITEMA, C., **DNS Extensions to support IP version 6, RFC 1886,** Março 1995 – Disponível em: <http://www.ietf.org/rfc/rfc1886.txt>. Acesso em mar 2013.

[14]Hawkinson,J., Bates, T.**Guidelines for creation, selection, and registration of an Autonomous System (AS), RFC1930,** Março 1996 - Disponível em: <http://www.ietf.org/rfc/rfc1930.txt> . Acesso em mar. 2013.

[15] **PoP-RJ** (O Ponto de Presença da Rede Nacional de Pesquisa (RNP), no Rio de Janeiro) Disponível em: <http://www.pop-rj.rnp.br/> . Acesso em mar. 2013.

[16] John J. Amoss, Dan Minoli., **Handbook of IPv4 to IPv6 transition : methodologies for institutional and corporate networks**. New York: Auerbach Publications, 2008.

[17] Internet System Consortium (ISC), **BIND 9 Administrator Reference Manual**. Redwood City, 2010.